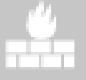
G DATA
SECURITY SOFTWARE







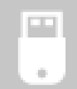
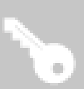









Table des matières

Premier démarrage

Nous vous remercions d'avoir opté pour notre produit et nous espérons que votre nouveau logiciel G DATA vous apportera entière satisfaction. Si vous ne parvenez pas à exécuter certaines procédures du premier coup, vous trouverez de l'aide dans notre documentation. Si vous avez des questions, vous pouvez contacter les experts du **ServiceCenter**.

> **Remarque** : Vous pouvez à tout moment activer l'aide du programme dans le logiciel et obtenir directement toutes les informations nécessaires. Pour ce faire, il vous suffit de cliquer sur l'icône d'aide dans le programme.

ServiceCenter

L'installation et l'utilisation du logiciel G DATA sont en règle générale simples et évidentes. En cas de problèmes, vous pouvez cependant facilement contacter les collaborateurs compétents de notre ServiceCenter :

> **www.gdata.fr** / **www.gdata.be** / **www.gdata.ch**

Installation

Pour que le logiciel fonctionne sans aucun problème, votre ordinateur doit correspondre à l'une des configurations minimales suivantes, en fonction du système d'exploitation :

- Microsoft Windows 8.1/Windows 8/Windows 7/Windows Vista (32/64 bits), 1 Go d'espace mémoire disponible
- Microsoft Windows XP (version SP2 ou supérieure, 32 bits), 512 Mo d'espace mémoire disponible

Si votre ordinateur est tout neuf ou s'il était jusqu'à présent protégé par un logiciel antivirus, vous pouvez procéder à l'installation comme suit. Si vous avez des raisons de penser que votre ordinateur est infecté, nous vous recommandons de procéder, avant installation du logiciel, à une analyse **BootScan**.

> **Attention** : si vous utilisiez jusqu'à présent le logiciel antivirus d'un autre fabricant, vous devez le supprimer complètement de votre ordinateur. Les logiciels antivirus sont ancrés très profondément dans la structure du système Windows, nous vous conseillons donc de procéder à la désinstallation du logiciel mais également d'utiliser, si possible, les outils de nettoyage mis à disposition par le fabricant dans son centre d'assistance en ligne.

Étape 1 - lancement de l'installation

Veuillez procéder comme suit pour lancer l'installation :

- **Installation à l'aide du CD/DVD** : pour commencer l'installation, insérez le CD ou DVD du programme.
- **Téléchargement du logiciel** : pour commencer l'installation de la version du logiciel téléchargée sur Internet, il vous suffit de double-cliquer sur le fichier téléchargé.

Une fenêtre d'installation s'affiche alors automatiquement.

> **Remarque** : si l'installation ne démarre pas : il est possible que la fonction de démarrage automatique de votre ordinateur ne soit pas correctement configurée. Le logiciel ne peut alors pas démarrer automatiquement le processus d'installation une fois le CD du programme inséré. Aucune fenêtre d'installation du logiciel G DATA ne s'affiche.
>
> - Si une fenêtre de sélection de lecture automatique s'affiche à la place, veuillez cliquer sur l'option **Exécuter AUTOSTRT.EXE**.
> - Si aucune fenêtre de sélection ne s'affiche, veuillez rechercher le support de données sur lequel le logiciel G DATA se trouve dans l'Explorateur Windows. Lancez ensuite le fichier **Setup** ou **Setup.exe**.

Étape 2 - sélection de la langue

Veuillez maintenant sélectionner la langue dans laquelle vous souhaitez installer le nouveau logiciel G DATA.

Étape 3 - mode d'installation

Un assistant vous accompagne maintenant dans la procédure d'installation du logiciel sur votre ordinateur. Veuillez indiquer si vous souhaitez procéder à une installation standard ou à une installation définie par l'utilisateur. Nous vous recommandons d'opter pour une installation standard.

Initiative d'information sur les logiciels malveillants : les laboratoires de sécurité de G DATA recherchent constamment des moyens de protéger les clients de G DATA des logiciels malveillants (virus, vers et programmes nuisibles). Plus les informations abondent, plus les mécanismes de protection développés peuvent être efficaces. De nombreuses informations ne sont toutefois disponibles que sur les systèmes attaqués ou contaminés. Pour que ces informations puissent également être prises en compte dans les analyses, G DATA a lancé l'initiative d'information sur les logiciels malveillants. Dans ce cadre, les informations relatives aux logiciels malveillants sont envoyées aux laboratoires de sécurité de G DATA. De par votre participation, vous contribuez à une utilisation encore plus sûre d'Internet pour tous les clients de G DATA. Lors de l'installation du logiciel G DATA, vous pouvez déterminer si les informations destinées aux laboratoires de sécurité de G DATA doivent être ou non mises à disposition.

> **Remarque** : Dans le cadre de l'installation définie par l'utilisateur, vous pouvez sélectionner l'emplacement d'enregistrement des données du programme et indiquer les modules logiciels (protection contre le pollupostage, par exemple) qui doivent être installés.

Étape 4 - contrat de licence

Veuillez maintenant lire et accepter le contrat de licence.

Étape 5 - installation définie par l'utilisateur (en option)

Si vous avez opté pour l'installation définie par l'utilisateur, deux fenêtres d'assistant s'affichent maintenant. Elles vous permettent de sélectionner le répertoire d'installation du logiciel et les modules à installer. Si vous avez opté pour l'installation standard, vous pouvez ignorer cette étape.

- **Défini par l'utilisateur** : vous pouvez indiquer ici le contenu de l'installation en activant les cases à cocher des différents modules logiciels (AntiSpam, etc.).
- **Complète** : tous les modules de la version du logiciel sont installés.
- **Minimale** : seule la protection antivirus de base de votre logiciel G DATA est installée avec le module AntiVirus.

> **Actualisations** : vous pouvez à tout moment installer des modules logiciels supplémentaires ou mettre le logiciel à jour via le programme d'installation. Pour ce faire, il vous suffit de démarrer le programme d'installation et de sélectionner **Modifier l'installation** pour ajouter ou supprimer des modules. Si vous disposez d'une nouvelle version du programme et souhaitez actualiser la version, l'option **Actualisation définie par l'utilisateur** vous permet de sélectionner les nouveaux modules à installer.

Étape 6 - version du logiciel

Vous pouvez maintenant indiquer ici si vous souhaitez installer le logiciel en tant que version complète ou version d'essai. Si vous avez acheté le logiciel et disposez d'un numéro d'enregistrement, vous devez bien évidemment sélectionner l'option **Version complète**. Vous pouvez également profiter de notre accès d'essai, limité dans le temps, pour découvrir gratuitement le logiciel de G DATA.

Étape 7 - activation du produit

L'activation du produit a lieu lors de l'installation. Cette procédure vous permet d'activer le logiciel.

- **Saisir un nouveau numéro d'enregistrement** : lors de la réinstallation du logiciel G DATA, sélectionnez cette option et saisissez le numéro d'enregistrement qui accompagne le produit. Selon le type de produit, il est indiqué au verso du manuel d'utilisation, dans le courrier de confirmation du téléchargement du logiciel ou sur l'étui du CD.

  > **Remarque** : La saisie du numéro d'enregistrement vous permet d'activer le produit et d'obtenir vos données d'accès, pour utilisation ultérieure, par courrier électronique.

- **Saisir les données d'accès** : lors de l'activation du logiciel G DATA, vous recevez des données d'accès (nom d'utilisateur et mot de passe). Pour réinstaller le logiciel ou ajouter d'autres ordinateurs dans le cadre d'une licence multipostes, il vous suffit de saisir les données d'accès ici.

  > **Remarque** : vous recevez les données d'accès par courrier électronique. Les données d'accès ne sont pas fournies avec le produit.
  >
  > Si vous avez égaré ou oublié vos codes d'accès, lors de l'enregistrement, cliquez sur l'entrée **Vous avez oublié vos données d'accès ?**. Une page Web dans laquelle vous pouvez de nouveau saisir votre numéro d'enregistrement s'affiche. Une fois le numéro saisi, les données d'accès vous sont envoyées à l'adresse électronique indiquée lors de l'enregistrement. Si vous avez changé d'adresse électronique depuis, veuillez vous adresser à notre **ServiceCenter**.

- **Activer ultérieurement** : si vous souhaitez uniquement jeter un œil au logiciel, vous pouvez également l'installer sans saisir les données. Cette forme de programme ne charge pas les mises à jour Internet, aucune protection n'est donc assurée contre les logiciels malveillants. Vous pouvez saisir votre numéro d'enregistrement ou vos données d'accès à tout moment par la suite,

lorsque vous procédez à une mise à jour.

Étape 8 - finalisation de l’installation

Vous devez éventuellement redémarrer votre ordinateur une fois l’installation terminée. Le logiciel G DATA est ensuite à votre disposition.

Après l’installation

Après installation, vous pouvez lancer le logiciel G DATA que vous venez d’installer à l’aide de l’icône de programme dans la barre de tâches. Des fonctions de sécurité supplémentaires sont désormais disponibles sur votre ordinateur :



Icône de sécurité : votre logiciel G DATA assure la protection permanente de votre ordinateur contre les logiciels malveillants et les attaques. La présence de l'icône dans la barre des tâches de votre ordinateur vous indique que le logiciel nécessite une intervention de l’utilisateur. Cliquez avec le bouton droit de la souris sur l’icône pour ouvrir l’interface du programme G DATA. Veuillez également lire à ce propos le chapitre **Icône de sécurité**.



Destructeur : si vous avez sélectionné l’application de destruction de fichiers lors de l’installation (non intégrée à l’application G DATA AntiVirus), elle est disponible sous forme d’icône de bureau. Les données placées dans l’application de destruction de fichiers sont supprimées de manière à ne pas pouvoir être récupérées, même à l’aide d’outils de récupération des données professionnels.

Vérification rapide : la vérification rapide vous permet de vérifier les fichiers facilement, sans démarrer le logiciel. Il vous suffit de sélectionner les fichiers ou les dossiers, dans l’Explorateur Windows, par exemple, à l’aide de la souris. Cliquez maintenant avec le bouton droit de la souris et sélectionnez **Analyse antivirus** dans la boîte de dialogue qui s’affiche. Une analyse antivirus est alors automatiquement effectuée au niveau des fichiers correspondants.

Votre ordinateur ne démarre pas comme d’habitude après installation du logiciel : il est possible que le CD du programme se trouve encore dans le lecteur. Il vous suffit de retirer le CD, l’ordinateur démarrera de la manière habituelle.

SecurityCenter

Vous n'avez besoin d'activer le SecurityCenter que lorsque vous souhaitez intervenir activement sur l'une des nombreuses fonctions supplémentaires du logiciel. Votre ordinateur est protégé en permanence contre les virus et autres menaces en arrière-plan. Si le logiciel a besoin de votre intervention, vous en êtes automatiquement informé par un message dans la barre des tâches de votre ordinateur.

Statut de sécurité

 Le système est protégé dans la mesure où une coche verte apparaît à côté de l'entrée **Statut de sécurité**.

 Un point d'exclamation rouge indique que le système est exposé à un danger immédiat. Vous devez lancer immédiatement les mesures permettant de protéger vos données.

 L'icône du caractère générique s'affiche pour vous indiquer que la fonction de sécurité correspondante (protection anti-pollupostage, par exemple) n'a pas été activée.

 Une icône jaune indique qu'une intervention rapide de l'utilisateur est requise, lorsqu'une mise à jour du programme du logiciel est disponible, par exemple.

L'ensemble des fonctions et rubriques du programme (**Protection antivirus** ou **Paramètres**, par exemple) peut être utilisé lorsque vous êtes activement impliqué dans la sécurité du système. Cela n'est cependant pas une obligation ! Vous êtes libre de choisir votre degré d'intervention dans la protection antivirus et la sauvegarde des données du système. Une aide complète est disponible dans le logiciel.

Principales fonctions

Les icônes suivantes indiquent le statut de sécurité de la rubrique correspondante.

 **Paramètres :** ce bouton situé en haut à droite vous permet d'accéder à toutes les boîtes de dialogue de paramétrage des différentes rubriques du logiciel. Vous avez également la possibilité, dans chaque rubrique, de sélectionner directement la boîte de dialogue de paramétrage correspondante.

 **Protocoles** : le logiciel répertorie ici les protocoles de toutes les actions effectuées (vérifications antivirus, mises à jour, virus détectés, etc.).

 Les fonctions suivantes sont également disponibles dans la partie supérieure droite de l'en-tête du logiciel :

Afficher l'aide : vous pouvez à tout moment consulter l'aide du programme détaillée dans le logiciel. Pour ce faire, il vous suffit de cliquer sur le bouton d'aide indiqué dans le programme.

Mettre le programme à jour : si de nouvelles versions du programme sont disponibles, vous pouvez mettre le logiciel à jour, tout comme les informations antivirus, en un clic de souris. Si vous êtes informé de l'existence d'une mise à jour, il vous suffit de cliquer sur l'entrée Mettre le programme à jour. Pour de plus amples informations, reportez-vous à la section : **Mises à jour**

Infos : vous obtenez ici des informations relatives à la version du programme. Le numéro de version peut notamment être utile lorsque vous contactez le **ServiceCenter** .

Affichage du statut

Les statuts suivants vous indiquent le statut de sécurité de votre système. Lorsque vous cliquez sur une entrée, vous pouvez immédiatement lancer des actions permettant d'optimiser le statut de sécurité :

Protection temps réel

La protection antivirus en temps réel analyse l'ensemble de votre ordinateur à la recherche de virus ; elle contrôle les procédures d'écriture et de lecture et dès qu'un programme souhaite exécuter des fonctions nuisibles ou diffuser des fichiers malveillants, il est bloqué par la protection antivirus. Le gardien est votre principale protection ! La protection antivirus ne doit jamais être désactivée !

- **Désactiver le gardien** : si vous souhaitez néanmoins désactiver la protection antivirus, vous pouvez exécuter la procédure nécessaire ici. Si vous souhaitez optimiser les performances de votre ordinateur en désactivant la protection antivirus, vérifiez impérativement qu'il ne vous est pas possible d'obtenir le résultat souhaité en modifiant les paramètres de la protection antivirus. Vous avez pour cela la possibilité de modifier les paramètres de manière adaptée lors de la désactivation de la protection antivirus. Cliquez pour ce faire sur **Modifier la sécurité/les performances** et suivez les consignes du chapitre d'aide du même nom. Vous pouvez aussi

désactiver complètement la protection antivirus.

- **Désactiver la surveillance comportementale** : la surveillance comportementale est un système de détection intelligente des logiciels malveillants inconnus, il s'agit d'une protection complémentaire, qui fonctionne indépendamment des signatures antivirus. La surveillance comportementale doit généralement être activée.

- **Autres paramètres** : vous retrouverez de plus amples informations à ce sujet dans le chapitre **Paramètres | AntiVirus | Protection temps réel**.

Dernière analyse en cas d'inactivité

Ici s'affiche la date de la dernière analyse antivirus complète de votre ordinateur. Si cette entrée s'affiche en rouge, vous devez procéder à une analyse antivirus assez rapidement.

- **Analyser l'ordinateur** : si vous avez le temps et que vous ne souhaitez pas utiliser l'ordinateur dans les heures qui suivent, vous pouvez lancer ici une vérification complète de l'ordinateur. Vous pouvez utiliser l'ordinateur pendant l'analyse. La vérification antivirus effectuée étant cependant basée sur des performances maximales, il est possible que les autres applications soient plus lentes. Davantage d'informations sont disponibles à ce sujet au chapitre **Analyse antivirus**.

- **Avancer l'analyse ScanDiscret** : l'analyse en cas d'inactivité démarre automatiquement lorsque l'ordinateur est inactif et procède à une vérification complète de l'ordinateur à intervalles automatiquement définis. Si vous souhaitez procéder à un scan discret avant la prochaine échéance définie automatiquement, sélectionnez **Démarrer l'analyse en cas d'inactivité maintenant**. Si vous ne souhaitez pas que le logiciel G Data procède automatiquement à une analyse en cas d'inactivité lorsque vous interrompez votre travail, vous pouvez également désactiver cette fonction sous **Désactiver ScanDiscret** (déconseillé).

Pare-feu

Le pare-feu protège votre ordinateur de l'*espionnage*. Il vérifie les données et les programmes qui accèdent à votre ordinateur à partir d'Internet ou d'un réseau, ainsi que les données envoyées par votre ordinateur. Dès qu'il apparaît que des données doivent être transférées ou téléchargées sur votre ordinateur sans autorisation préalable, l'alerte du pare-feu intervient et bloque l'échange de données non autorisé. Ce module logiciel est intégré aux programmes G DATA InternetSecurity et G DATA TotalProtection.

- **Désactiver le pare-feu** : Vous pouvez également désactiver le pare-feu si nécessaire. Dans ce cas, votre ordinateur reste connecté à Internet et aux autres réseaux, mais n'est plus protégé par le pare-feu contre les attaques ou les tentatives d'espionnage (déconseillé).

- **Désactiver le pilote automatique** : en règle générale, il est recommandé d'utiliser le pare-feu en mode **pilote automatique**. Il s'exécute quasiment en arrière-plan et vous protège sans que vous ayez à procéder à d'importants paramétrages. Si vous utilisez le pare-feu sans le pilote automatique, une boîte de dialogue vous permettant d'optimiser le pare-feu progressivement, en fonction des réalités de votre système, s'affiche en cas de doutes. Il s'agit d'une fonction utile pour les utilisateurs expérimentés. Il n'est toutefois pas recommandé de désactiver le pilote automatique en temps normal.

- **Autres paramètres** : vous retrouverez de plus amples informations à ce sujet dans le chapitre **Paramètres | Pare-feu | Automatique**.

Protection Internet

Cette rubrique vous permet d'activer ou de désactiver le protection Internet. La protection Internet est un module qui détecte et désactive automatiquement les menaces lors de la navigation sur Internet et lors des téléchargements. Il s'agit d'un complément utile à l'outil de surveillance antivirus, qui bloque les sites Web et les téléchargements nuisibles avant même qu'ils ne soient activés.

Si le logiciel G DATA détecte un site Internet en tant que menace et le bloque, le navigateur affiche une page d'information de G DATA à la place du site Web.

- **Désactiver la protection Internet** : la désactivation de la protection Internet peut représenter un gain de temps lors des téléchargements volumineux depuis une source sûre, par exemple. En principe, lorsque la protection Internet est désactivée, l'ordinateur est protégé par l'outil de surveillance antivirus. Vous ne devez cependant renoncer à la protection Internet que de manière exceptionnelle.

- **Déterminer exceptions** : la protection Internet se charge de vous éviter de devenir victime de pages Web infectées ou frauduleuses. Dans de rares cas, il peut aussi arriver qu'une page Internet ne soit pas présentée correctement, bien qu'elle provienne d'un fournisseur sûr. Dans un tel cas, vous pouvez alors placer cette adresse Internet dans la liste blanche, c'est-à-dire que vous pouvez la définir comme exception et que la protection Internet ne bloquera plus cette page. Reportez-vous au chapitre **Déterminer exceptions**pour connaître la procédure.

- **Autres paramètres** : vous retrouverez de plus amples informations à ce sujet dans le chapitre **Paramètres | AntiVirus | Protection Internet**.

Analyse de la messagerie électronique

La fonction d'analyse du courrier électronique vous permet de vérifier la présence de virus dans les courriers électroniques entrants et sortants ainsi que dans leurs pièces jointes et d'éliminer ainsi les infections éventuelles directement à la source. Si un virus est détecté dans une pièce jointe, le logiciel peut le supprimer ou réparer les fichiers infectés.

- **Désactiver la protection des courriers électroniques** : sélectionnez cette option si vous ne souhaitez pas que votre logiciel G DATAvérifie les courriers électroniques. La désactivation de cette fonction représente toutefois un risque plus élevé pour la sécurité et ne doit avoir lieu que de manière exceptionnelle.

- **Autres paramètres** : vous retrouverez de plus amples informations à ce sujet dans le chapitre **Paramètres | AntiVirus | Analyse des messages électroniques**.

Microsoft Outlook : l'analyse des courriers électroniques repose ici sur un plugiciel. Ce dernier offre la même sécurité que la fonction de protection des programmes de messagerie POP3/IMAP dans les options antiVirus. Une fois ce plugiciel installé, le menu Outlook Outils inclut la fonction **Rechercher des virus dans un dossier**, qui vous permet de vérifier que les dossiers de messages ne sont pas infectés.

Protection contre le pollupostage

Offres spéciales, publicité et lettres d'information – le flot de courriers électroniques indésirables ne cesse de croître. Votre boîte aux lettres déborde-t-elle de ces quantités innombrables de courriers électroniques indésirables ? Le logiciel G DATA protège du pollupostage, bloque efficacement les expéditeurs de pollupostage et empêche les caractéristiques falsifiées grâce à l'association de critères de vérification anti-pollupostage modernes. Ce module logiciel est intégré aux programmes G DATA InternetSecurity et G DATA TotalProtection.

- **Protocole : Spam**: cette rubrique vous propose un aperçu de tous les courriers électroniques considérés comme du pollupostage par le logiciel G DATA. Le bouton **Actualiser** vous permet d'interroger les données du logiciel tandis que le bouton **Supprimer** supprime toutes les entrées sélectionnées. Les véritables courriers électroniques se trouvant dans votre programme de messagerie électronique ne seront évidemment pas supprimés. Le bouton **Sur liste blanche** vous permet de placer dans la liste blanche un courrier électronique sélectionné afin d'exclure l'adresse électronique concernée des prochaines vérifications anti-pollupostage. Le bouton **Sur liste noire** vous permet de placer dans la liste noire un courrier électronique sélectionné afin que l'adresse concernée soit particulièrement contrôlée lors des prochaines vérifications anti-pollupostage.

- **Protocole : Pas de spam** : cette rubrique vous propose un aperçu de tous les courriers électroniques non considérés comme du pollupostage par le logiciel G DATA. Le bouton **Actualiser** vous permet d'interroger les données du logiciel tandis que le bouton **Supprimer** supprime toutes les entrées sélectionnées. Les véritables courriers électroniques se trouvant dans votre programme de messagerie électronique ne seront évidemment pas supprimés. Le bouton **Sur liste blanche** vous permet de placer dans la liste blanche un courrier électronique sélectionné afin d'exclure l'adresse électronique concernée des prochaines vérifications anti-pollupostage. Le bouton **Sur liste noire** vous permet de placer dans la liste noire un courrier électronique sélectionné afin que l'adresse concernée soit particulièrement contrôlée lors des prochaines vérifications anti-pollupostage.

- **Modifier la liste blanche** : La liste blanche vous permet d'exclure explicitement de la vérification des spams les adresses de certains expéditeurs ou de certains domaines. Pour ce faire, il vous suffit de cliquer sur le bouton **Nouveau** et de saisir, dans le champ **Adresses/domaines**, les adresses électroniques (lettre d'information@site d'information.fr, par exemple) ou les domaines (site d'information.fr, par exemple) que vous ne souhaitez pas prendre en compte dans le cadre de la suspicion de pollupostage. Le logiciel G DATA ne traite alors pas les courriers électroniques de l'expéditeur ou du domaine d'expéditeurs comme du pollupostage. Le bouton Importer vous permet d'ajouter à la liste blanche des listes prédéfinies d'adresses électroniques ou de domaines. Les adresses et les domaines de ces listes doivent se présenter l'un en-dessous de l'autre dans des lignes individuelles. Le format utilisé est celui d'un simple fichier texte, pouvant, par exemple, être créé avec l'outil Bloc-notes de Windows. Le bouton **Exporter** vous permet d'exporter une telle liste blanche sous la forme d'un fichier texte.

- **Modifier la liste noire** : la liste noire vous permet de définir explicitement comme étant du pollupostage les messages provenant des adresses de certains expéditeurs ou de certains domaines. Pour ce faire, il vous suffit de cliquer sur le bouton **Nouveau** et de saisir, dans le champ **Adresses/domaines**, les adresses électroniques (lettre d'information@megaspam.fr.vu, par exemple) ou les domaines (megaspam.fr.vu, par exemple) que vous souhaitez prendre en compte dans le cadre de la suspicion de pollupostage. Le logiciel G DATA traite alors les courriers électroniques de l'expéditeur ou du domaine d'expéditeurs comme des courriers présentant une probabilité élevée de pollupostage. Le bouton **Importer** vous permet d'ajouter à la liste noire des listes prédéfinies d'adresses électroniques ou de domaines. Les adresses et les domaines de ces listes doivent se présenter l'un en-dessous de l'autre dans des lignes individuelles. Le format utilisé est celui d'un simple fichier texte, pouvant, par exemple, être créé avec l'outil Bloc-notes de Windows. Le bouton **Exporter** vous permet d'exporter la liste noire en tant que fichier texte.

- **Désactiver la protection antispam** : si nécessaire, vous pouvez désactiver ici la protection anti-pollupostage de votre ordinateur, si vous n'avez pas encore installé de programme de messagerie électronique sur votre ordinateur, par exemple.

- **Autres paramètres** : vous retrouverez de plus amples informations à ce sujet dans le chapitre **Paramètres | AntiSpam | Filtre**

antispam.

Dernière mise à jour

La date à laquelle votre ordinateur a obtenu des signatures antivirus depuis Internet pour la dernière fois s'affiche ici. Si cette entrée s'affiche en rouge, vous devez effectuer une mise à jour antivirus relativement rapidement. Il vous suffit de cliquer sur l'entrée et de sélectionner l'option **Mettre les signatures antivirus à jour**.

- **Mettre les signatures antivirus à jour** : les mises à jour des signatures antivirus sont normalement effectuées de manière automatique. Cliquez sur ce bouton si vous avez besoin de procéder immédiatement à une mise à jour.
- **Désactiver les mises à jour automatiques** : désactivez cette option si vous ne souhaitez pas que le logiciel G DATA se charge automatiquement de la mise à jour des signatures antivirus. La désactivation de cette fonction représente toutefois un risque plus élevé pour la sécurité et ne doit avoir lieu que de manière exceptionnelle.
- **Autres paramètres** : vous retrouverez de plus amples informations à ce sujet dans le chapitre **Paramètres | AntiVirus | Mises à jour**.

Prochaine mise à jour

cette entrée vous indique quand la prochaine mise à jour doit avoir lieu. Si vous souhaitez procéder immédiatement à une mise à jour, il vous suffit de cliquer sur l'entrée et de sélectionner l'option **Mettre les signatures antivirus à jour**.

- **Mettre les signatures antivirus à jour** : les mises à jour des signatures antivirus sont normalement effectuées de manière automatique. Cliquez sur ce bouton si vous avez besoin de procéder immédiatement à une mise à jour.
- **Désactiver les mises à jour automatiques** : désactivez cette option si vous ne souhaitez pas que le logiciel G DATA se charge automatiquement de la mise à jour des signatures antivirus. La désactivation de cette fonction représente toutefois un risque plus élevé pour la sécurité et ne doit avoir lieu que de manière exceptionnelle.
- **Autres paramètres** : vous retrouverez de plus amples informations à ce sujet dans le chapitre **Paramètres | AntiVirus | Mises à jour**.

Licence

La durée de validité de la licence de mise à jour antivirus est affichée sous l'entrée **Licence**, sur la page de gauche de l'interface du programme. Aucun logiciel n'a un besoin si important d'actualisations permanentes que les logiciels antivirus. Avant que votre licence n'expire, le logiciel vous rappelle automatiquement que vous devez la prolonger. De manière pratique et facile, via Internet !

Afficher les informations relatives à la licence

Si vous cliquez sur le champ d'information dans la rubrique Licence, un champ avec votre nom d'utilisateur et votre clé de licence s'affiche. Si vous avez des questions au sujet de votre licence, le **ServiceCenter G DATA** peut vous aider de manière ciblée à l'aide de ces informations. Si vous avez oublié votre mot de passe, vous pouvez générer rapidement et facilement un nouveau mot de passe à l'aide de ce champ.

Protéger davantage de PC/Étendre les fonctionnalités

Bien évidemment, il est possible à tout moment d'augmenter le nombre de vos licences ou de réaliser une mise à niveau sur des produits dotés de fonctionnalités étendues. Si vous cliquez sur l'entrée **Protéger davantage d'ordinateurs PC** dans SecurityCenter, vous êtes automatiquement redirigé vers le site Web de notre boutique en ligne. L'option **Etendre les fonctionnalités** vous permet d'accéder à notre Upgrade-Center, dans lequel vous pouvez également commander des fonctionnalités étendues pour nos autres versions logicielles, à des conditions spécifiques.

Que se passe-t-il lors de l'expiration de ma licence ?

Quelques jours avant l'expiration de votre licence, une fenêtre d'informations s'affiche dans la barre des tâches. Cliquez dessus pour afficher une boîte de dialogue qui vous permet de prolonger votre licence sans problème et en quelques étapes. Il vous suffit de cliquer sur le bouton **Acheter maintenant** et de saisir les données vous concernant. Votre protection antivirus est alors immédiatement garantie. Vous recevrez la facture, dans les jours suivants, par la poste.

> **Remarque** : Cette boîte de dialogue ne s'affiche qu'au bout de la première année. Votre licence est ensuite automatiquement prolongée chaque année. Vous pouvez toutefois résilier à tout moment cet abonnement sans fournir aucune raison.

Modules logiciels

Selon le logiciel installé, les modules logiciels suivants sont à votre disposition :



SecurityCenter : votre centre de sécurité personnel. Vous retrouverez ici toutes les informations nécessaires à la protection de votre ordinateur contre les logiciels malveillants. Vous pouvez ainsi réagir de manière ciblée aux menaces.



Protection antivirus : cette rubrique comprend des informations relatives à la dernière analyse antivirus de l'ordinateur et vous permet de savoir si la protection antivirus est actuellement activée. Vous pouvez également vérifier que l'ordinateur ou les supports de données ne sont pas infectés par des logiciels malveillants, traiter les fichiers infectés placés en quarantaine et créer un support d'amorçage.



Pare-feu : le pare-feu protège votre ordinateur de l'espionnage. Il vérifie les données et les programmes qui accèdent à votre ordinateur à partir d'Internet ou d'un réseau, ainsi que les données envoyées par votre ordinateur. Dès qu'il apparaît que des données doivent être transférées ou téléchargées sur votre ordinateur sans autorisation préalable, l'alerte du pare-feu intervient et bloque l'échange de données non autorisé. Ce module logiciel est intégré aux programmes G DATA InternetSecurity et G DATA TotalProtection.



Sauvegarde : avec la numérisation croissante de notre vie quotidienne, l'utilisation de services de musique en ligne, les appareils photo numériques et la correspondance électronique, la sécurisation des données personnelles représente un enjeu de plus en plus important. Que ce soit en raison d'erreurs matérielles, de mégardes possibles ou de dommages causés par des virus ou des attaques de pirates, il faut régulièrement sécuriser vos documents personnels. Le module de sauvegarde effectue cette opération à votre place et protège ainsi vos documents et vos fichiers les plus importants, sans que vous ayez à vous en préoccuper. Ce module logiciel est intégré au programme G DATA TotalProtection.



Tuner : qu'il s'agisse de rappels automatiques de mises à jour Windows, de défragmentations programmées à fréquence régulière, du nettoyage régulier des entrées caduques du registre ou des fichiers temporaires, le tuner vous offre un outil d'accélération et de simplification de votre système Windows. Ce module logiciel est intégré au programme G DATA TotalProtection.



Contrôle parental : le contrôle parental vous permet de réguler l'utilisation d'Internet et de l'ordinateur par vos enfants. Ce module logiciel est intégré aux programmes G DATA InternetSecurity et G DATA TotalProtection.



Autostart Manager : l'application Autostart Manager permet de gérer les programmes automatiquement lancés au démarrage de Windows. Ces programmes sont normalement directement chargés au démarrage du système. S'ils sont gérés dans l'application Autostart Manager, ils peuvent être lancés de manière retardée ou en fonction de la charge du système ou du disque dur. Cela permet de démarrer plus rapidement le système et d'améliorer ainsi les performances de l'ordinateur.



Contrôle des périphériques : cette fonction vous permet de limiter l'utilisation de périphériques comme les supports de données amovibles, les lecteurs de CD/DVD et les lecteurs de disquettes pour certains utilisateurs de votre ordinateur. Vous pouvez ainsi interdire l'exportation ou l'importation de données ou l'installation de logiciels.

Protection antivirus

Ce module vous permet de vérifier de manière ciblée que votre ordinateur ou des supports de données sélectionnés ne sont pas infectés par des logiciels nuisibles. Cette vérification est recommandée lorsque vous recevez des clés USB ou des CD gravés d'amis, de parents ou de collègues de travail, par exemple. La vérification antivirus est également recommandée lors de l'installation de nouveaux logiciels et lors de téléchargements depuis Internet.

> **Attention** : la vérification de l'ordinateur ou des supports de données sélectionnés est une protection supplémentaire. Vous êtes en principe protégé de manière optimale contre les menaces que présentent les logiciels nuisibles avec l'analyse en cas d'inactivité G Data et la protection antivirus G DATA, toujours activée en arrière-plan. Une vérification antivirus sera également en mesure de trouver des virus qui auraient été copiés sur votre ordinateur avant que vous n'ayez installé le logiciel G DATA ou qui se seraient greffés sur votre ordinateur alors que la protection antivirus n'était pas encore activée.

Analyse antivirus

Sélectionnez ici les zones de votre ordinateur ou les supports de données qui doivent être vérifiés de manière ciblée :



Vérifier l'ordinateur (tous les disques durs locaux) : si vous voulez analyser votre ordinateur indépendamment de la vérification automatique par le biais de l'analyse en cas d'inactivité (parce que vous soupçonnez la présence d'un virus, par exemple), il vous suffit de cliquer sur cette entrée. Votre ordinateur effectue alors une vérification antivirus. Veuillez également lire à ce propos le chapitre suivant : **Exécuter l'analyse antivirus**



Vérifier la mémoire et la fonction de démarrage automatique : l'ensemble des processus des fichiers programmes et des DLL (bibliothèques de programmes) en cours d'exécution est alors vérifié. Les programmes malveillants peuvent être ainsi directement supprimés de la mémoire et de la zone de démarrage automatique. Les virus actifs peuvent ainsi être directement supprimés sans qu'il soit nécessaire de contrôler la totalité du disque dur. Cette fonction ne remplace pas l'analyse antivirus régulière des données enregistrées, mais l'analyse antivirus complète.



Vérifier les répertoires/fichiers : analyse les lecteurs, dossiers ou fichiers sélectionnés. Lorsque vous cliquez sur cette action, une sélection de répertoires et de fichiers s'ouvre. Vous pouvez ainsi vérifier des fichiers isolés, mais également des répertoires complets. Dans l'arborescence des répertoires, vous pouvez sélectionner et ouvrir des répertoires, dont le contenu sera ensuite affiché dans l'affichage des fichiers, en cliquant sur l'icône Plus. Tous les répertoires et fichiers dont la case à cocher est activée sont vérifiés par le logiciel.

Les dossiers, dont certains des fichiers ne doivent pas être analysés, sont signalés par une coche grisée.



Vérifier les supports amovibles : cette fonction permet d'analyser les CD-ROM, les DVD-ROM, les cartes mémoire et les clés USB. Si vous cliquez sur cette action, tous les supports amovibles connectés à votre ordinateur sont soumis à une analyse antivirus (donc également les CD et les cartes mémoire insérés, les disques durs USB ou les clés USB). Veuillez tenir compte du fait que le logiciel ne peut évidemment supprimer aucun virus sur les supports qui n'autorisent pas l'accès en écriture (CD-ROM gravés, par exemple). La détection de virus est alors enregistrée dans des rapports.



Détecter les RootKits : les trousses administrateur pirate tentent d'esquiver les méthodes de détection habituelles des virus. Vous pouvez, grâce à cette fonction, cibler votre recherche sur les trousses administrateur pirate sans effectuer une vérification complète des disques durs et des données enregistrées.

Fichiers en quarantaine

Vous pouvez choisir la manière dont doivent être traités les virus détectés au cours de l'analyse antivirus. L'une des options vous permet de mettre les fichiers infectés en quarantaine. La quarantaine est une zone protégée du logiciel, dans laquelle les fichiers infectés sont enregistrés sous forme cryptée de façon à empêcher la contamination des autres fichiers.



Afficher la quarantaine : la rubrique de la quarantaine s'affiche lorsque vous cliquez sur ce bouton.

Les fichiers mis en quarantaine restent dans l'état dans lequel le logiciel G DATA les a trouvés. Vous pouvez ensuite décider de ce que vous souhaitez faire.

- **Actualiser** : si la boîte de dialogue de la quarantaine est ouverte depuis un certain temps et qu'un virus a été détecté et placé en quarantaine (automatiquement, via le gardien, par exemple) depuis, vous pouvez actualiser l'affichage à l'aide de ce bouton.
- **Envoyer** : dans certains cas, vous pouvez envoyer à G DATA, via Internet, un fichier infecté qui ne peut pas être nettoyé. Le contenu

de ce fichier est traité bien évidemment en toute confidentialité. Les résultats de l'analyse sont intégrés à l'optimisation et à la mise à jour des signatures antivirus et du logiciel.

Initiative d'information sur les logiciels malveillants : les laboratoires de sécurité de G DATA recherchent constamment des moyens de protéger les clients de G DATA des logiciels malveillants (virus, vers et programmes nuisibles). Plus les informations abondent, plus les mécanismes de protection développés peuvent être efficaces. De nombreuses informations ne sont toutefois disponibles que sur les systèmes attaqués ou contaminés. Pour que ces informations puissent également être prises en compte dans les analyses, G DATA a lancé l'initiative d'information sur les logiciels malveillants. Dans ce cadre, les informations relatives aux logiciels malveillants sont envoyées aux laboratoires de sécurité de G DATA. De par votre participation, vous contribuez à une utilisation encore plus sûre d'Internet pour tous les clients de G DATA.

- **Désinfecter** : il est souvent possible de récupérer les fichiers infectés. Le logiciel supprime les éléments de virus dans le fichier infecté et reconstruit de cette manière le fichier d'origine non infecté. Si le programme parvient à nettoyer un fichier, il le restaure automatiquement à l'emplacement où il était enregistré avant l'analyse. Vous pouvez de nouveau y accéder sans restriction.
- **Retour** : il peut être parfois utile de restaurer à son emplacement d'origine un fichier infecté mis en quarantaine qui ne peut pas être nettoyé. Cela peut être effectué, par exemple, pour récupérer les données contenues dans le fichier. Nous vous conseillons de n'exécuter cette fonction que dans des cas exceptionnels et dans des conditions de sécurité strictes (par exemple, après avoir déconnecté l'ordinateur du réseau/d'Internet, après avoir sauvegardé les données non infectées, etc.).
- **Supprimer** : si vous n'avez plus besoin du fichier infecté, vous pouvez tout simplement le supprimer de la quarantaine.

Support d'amorçage

Le support d'amorçage est un outil très utile pour supprimer les virus des ordinateurs déjà contaminés. L'utilisation d'un support d'amorçage est recommandée sur les ordinateurs qui ne disposaient pas d'une protection antivirus avant installation du logiciel G Data. La procédure d'utilisation des **supports d'amorçage** est détaillée au chapitre **BootScan**.



Pour créer un support d'amorçage, il vous suffit de cliquer sur le bouton **Créer un support d'amorçage** et de suivre les instructions de l'assistant d'installation. Vous avez ici la possibilité de télécharger les dernières signatures antivirus pour mettre votre support d'amorçage à jour. Vous pouvez également choisir de graver le support d'amorçage sur un CD/DVD ou de l'utiliser sur une clé USB.

Restauration de la sauvegarde : si vous utilisez le programme G DATA TotalProtection, le support d'amorçage vous permet de rétablir la sauvegarde du lecteur sur le volume où se trouve actuellement le système. Il est également possible de rétablir une sauvegarde de lecteur ou de fichiers sur d'autres emplacements. Pour ce faire, insérez le support d'amorçage et sélectionnez la fonction **G DATA Backup (restauration)**.

Pare-feu

Le pare-feu protège votre ordinateur de l'*espionnage*. Il vérifie les données et les programmes qui accèdent à votre ordinateur à partir d'Internet ou d'un réseau, ainsi que les données envoyées par votre ordinateur.

Le module Pare-feu est constitué de trois rubriques :

- **État** : la zone État du module Pare-feu contient des informations de base concernant l'état actuel de votre système et du pare-feu.
- **Réseaux** : la rubrique Réseaux recense les réseaux (réseau local, réseau à distance, etc.) auxquels votre ordinateur est connecté.
- **Ensembles de règles** : cette rubrique vous permet de créer des règles spécifiques pour les différents réseaux et d'optimiser ainsi le fonctionnement du pare-feu.

Dès qu'il apparaît que des données doivent être transférées ou téléchargées sur votre ordinateur sans autorisation préalable, l'alerte du pare-feu intervient et bloque l'échange de données non autorisé.

 **Paramètres** : ce bouton situé en haut à droite vous permet d'accéder aux autres boîtes de dialogue de paramétrage du pare-feu.

État

La zone Statut du pare-feu contient des informations de base concernant l'état actuel de votre système et du pare-feu. Ces informations, disponibles sous forme de texte ou de chiffres, sont situées à droite de chaque élément d'information. L'état des composants est également représenté de manière graphique. Double-cliquez sur l'entrée correspondante pour exécuter directement des actions ou passer à la rubrique de programmes concernée.

Une fois la configuration d'un élément doté de l'icône d'avertissement optimisée, l'icône est remplacée par une coche verte dans la rubrique État.

- **Sécurité** : Quand vous utilisez votre ordinateur, le pare-feu note au fur et à mesure les programmes que vous utilisez pour accéder à Internet et ceux qui présentent ou pas un risque pour la sécurité du système. Selon votre connaissance de la technologie du pare-feu, vous pouvez le configurer de manière à ce qu'il vous offre un bon niveau de protection de base sans trop vous en occuper ou une protection de niveau professionnel adaptée à l'utilisation que vous faites de votre ordinateur, mais qui demande des connaissances plus approfondies. Vous pouvez définir le statut de sécurité ici : **Paramètres | Pare-feu | Automatique**.

- **Mode** : vous informe sur le paramètre de base d'exécution de votre pare-feu. Vous avez le choix entre la création manuelle ou la création automatique (pilote automatique) de règles.

  Pilote automatique : Le pare-feu travaille ici de manière entièrement autonome et tient les dangers automatiquement à distance de votre ordinateur domestique. Cette option offre une protection intégrale très pratique et est recommandée dans la plupart des cas. Le pilote automatique doit être activé par défaut.

  Autres paramètres : si vous souhaitez configurer votre pare-feu individuellement ou ne pas utiliser certaines applications avec le mode de pilote automatique, vous pouvez configurer votre propre protection de pare-feu via la création manuelle de règles. De plus amples informations sont disponibles au chapitre suivant : **Paramètres | Pare-feu | Automatique**.

- **Réseaux** : vous pouvez afficher ici les réseaux auxquels appartient votre ordinateur. De plus amples informations sont disponibles au chapitre suivant : **Pare-feu | Réseaux**.

- **Attaques repoussées** : dès que le pare-feu enregistre une attaque sur votre ordinateur, l'attaque est bloquée et enregistrée ici. Vous pouvez obtenir de plus amples informations en cliquant sur l'option de menu.

- **Radar d'applications** : cette boîte de dialogue vous indique les programmes momentanément bloqués par le pare-feu. Si vous souhaitez toutefois autoriser l'une des applications bloquées à exploiter le réseau, il suffit de la sélectionner et de cliquer sur le bouton **Autoriser**.

Réseaux

La rubrique Réseaux recense les réseaux (réseau local, réseau à distance, etc.) auxquels votre ordinateur est connecté. Elle indique également l'ensemble de règles (voir le chapitre Ensembles de règlesappliqué au réseau. Si vous décochez la case accompagnant un réseau, celui-ci n'est plus protégé par le pare-feu. Il est conseillé de ne désactiver la protection que dans des cas exceptionnels. Pour consulter ou modifier les paramètres de protection du pare-feu définis pour un réseau, sélectionnez le réseau et cliquez sur le bouton **Modifier**.

Modifier le réseau

Cette vue d'ensemble vous présente les informations et possibilités de paramétrage suivantes pour le réseau sélectionné :

- **Informations relatives au réseau** : affiche des informations relatives au réseau, telles que, le cas échéant, l'adresse IP, le masque de sous-réseau, la passerelle standard, le serveur DNS et le serveur WINS.
- **Pare-feu actif sur ce réseau** : Vous pouvez désactiver ici le pare-feu du réseau. Il est cependant conseillé de ne le faire que dans des cas exceptionnels.
- **Utilisation partagée de la connexion Internet** : dans le cas de connexions directes à Internet, vous pouvez déterminer ici si tous les ordinateurs reliés au réseau par un ordinateur connecté à Internet peuvent accéder à Internet ou non. Ce partage de connexion Internet (ICS) peut généralement être activé pour un réseau familial.
- **Autoriser les configurations automatiques (DHCP)** : une adresse IP dynamique est attribuée (via le protocole DHCP = Dynamic Host Configuration Protocol) lors de la connexion de votre ordinateur avec le réseau. Si vous êtes connecté au réseau via une configuration standard, vous devriez laisser cette case cochée.
- **Jeu de règles** : Vous pouvez choisir les jeux de règles prédéfinis et ainsi rapidement déterminer, sur la base des critères de surveillance du pare-feu, s'il s'agit d'un réseau de confiance, sensible ou à bloquer. Le bouton **Modifier le jeu de règles** vous permet en outre de configurer chaque jeu de règles séparément. Veuillez également lire à ce propos le chapitre Créer des jeux de règles.

Ensembles de règles

La rubrique Jeux de règles vous permet de créer des règles spécifiques pour les différents réseaux. Ces règles sont ensuite regroupées dans un jeu de règles. Des jeux de règles prédéfinies sont disponibles pour la connexion directe à Internet, les réseaux non fiables, les réseaux fiables et les réseaux à bloquer. L'aperçu affiche les différents jeux de règles avec leur nom. Les boutons **Nouveau**, **Supprimer** et **Modifier** permettent de modifier les jeux de règles existants ou d'en créer de nouveaux.

Les jeux de règles prédéfinis pour la **connexion directe à Internet**, **les réseaux fiables**, **les réseaux non fiables** et **les réseaux à bloquer** ne peuvent pas être supprimés. Vous pouvez en revanche supprimer à tout moment les jeux de règles que vous avez créés.

Créer des jeux de règles

Vous pouvez attribuer à chaque réseau son propre jeu de règles (ensemble de règles définies pour ce réseau). Vous pouvez ainsi moduler la protection du pare-feu en fonction du niveau de risque présenté par les réseaux. Par exemple, un réseau domestique requiert sans doute un niveau de protection moindre (et par conséquent, moins de travail d'administration) qu'un réseau d'accès à distance en contact direct avec Internet.

En outre, le bouton **Nouveau** permet également de créer un jeu de règles spécifique à chaque réseau. Dans la rubrique Jeux de règles, cliquez sur le bouton **Nouveau** et définissez les paramètres suivants dans la boîte de dialogue qui s'affiche :

- **Nom du jeu de règles** : attribuez ici un nom pertinent au jeu de règles.
- **Créer un jeu de règles vide** : vous pouvez créer ici un jeu de règles complètement vide et le remplir uniquement de règles que vous aurez définies.
- **Créer un jeu de règles incluant quelques règles utiles** : cette option vous permet d'intégrer au nouveau jeu de règles certaines règles de base prédéfinies pour les réseaux fiables, non fiables et à bloquer. Sur la base de ces préréglages, vous pouvez ensuite procéder à des modifications individuelles.

Le pare-feu met à votre disposition des jeux de règles prédéfinies applicables aux types de réseaux suivants :

- **Connexion directe à l'Internet** : les règles qui gèrent l'accès direct à Internet relèvent de cette catégorie.
- **Réseaux non fiables** : concerne généralement les réseaux ouverts qui accèdent à Internet, comme les réseaux à distance.

- **Réseaux fiables** : sont généralement considérés comme réseaux de confiance les réseaux domestiques et les réseaux d'entreprise.

- **Réseaux à bloquer** : utilisez cette option pour bloquer provisoirement ou définitivement l'accès de votre ordinateur à un réseau. Cela peut être utile, par exemple pour les connexions aux réseaux tiers dont on ne connaît pas bien le niveau de sécurité (tournois de jeux en réseau, réseaux d'entreprise externes, postes de travail publics, etc.).

Le nouveau jeu de règles apparaît dans la liste de la rubrique Jeux de règles sous le nom que vous lui avez attribué (par exemple, *Nouveau jeu de règles*). Si vous cliquez sur le bouton **Modifier**, le programme ouvre - selon les paramètres définis sous **Paramètres | Autres** (voir chapitre éponyme), l' assistant de règles ou lamode de modification avancé vous permettant de modifier les règles du jeu de règles s'affiche. Pour savoir comment ajouter des règles aux jeux de règles, reportez-vous à la section **Utilisation de l'assistant de règles** ou **Utilisation du mode de modification avancé**.

Il est également possible de créer des règles dans la boîte de dialogue d'information de l'alerte du pare-feu. Ce processus d'apprentissage est détaillé au chapitre **Alarme pare-feu** .

Utilisation de l'assistant de règles

L'assistant de règles vous permet d'ajouter de nouvelles règles ou de modifier les règles existantes d'un jeu de règles. Si vous ne connaissez pas bien la technologie de pare-feu, il est préférable de faire appel à l'assistant de règles du mode de modification avancé.

Dans l'assistant de règles, vous pouvez modifier une ou plusieurs règles du jeu de règles sélectionné. Vous créez donc toujours une règle à l'intérieur d'un jeu de règles contenant plusieurs règles.

Selon le jeu de règles défini pour un réseau, une application peut être bloquée dans un jeu de règles (par ex. pour les réseaux sensibles) et autorisée dans un autre (par ex. pour les réseaux de confiance). Vous pouvez ainsi définir des règles permettant à un navigateur d'accéder aux sites d'un réseau familial et lui interdisant d'accéder aux contenus provenant d'un réseau à distance.

L'assistant de règles vous propose les règles de base suivantes :

- **Autoriser ou bloquer les applications** : vous permet de sélectionner une application (programme) sur votre disque dur et de lui autoriser ou lui interdire expressément l'accès au réseau défini dans le jeu de règles. Pour cela, il vous suffit de sélectionner dans l'assistant le programme souhaité (**Chemin d'accès**) et d'indiquer, sous **Sens**, s'il doit être bloqué pour les connexions entrantes et/ou sortantes. Vous pouvez ainsi interdire à votre logiciel de lecteur MP3 de transmettre des données sur vos habitudes d'écoute (connexions sortantes) ou empêcher les mises à jour automatiques (connexions entrantes).

- **Autoriser ou bloquer les services réseau** : on entend par **port** une plage d'adresses donnée, chargée de transmettre automatiquement les données transférées via un réseau vers un protocole et un programme donnés. Par exemple, la transmission des sites Web habituels transite par le port 80, l'envoi des e-mails par le port 25 et la réception des e-mails par le port 110. Sans pare-feu, tous les ports sont généralement ouverts, bien que la majorité d'entre eux ne soient pas utilisés dans la plupart des cas. Le blocage d'un ou plusieurs ports peut donc permettre de combler des failles de sécurité que les hackers pourraient utiliser pour lancer des attaques. Remarque : l'Assistant vous permet de bloquer les ports de votre choix entièrement ou uniquement pour une application définie (votre lecteur MP3, par ex.).

- **Partage des fichiers et des imprimantes** : lorsque vous autorisez l'accès, vous avez la possibilité d'utiliser les dossiers et imprimantes partagés du réseau. D'autres ordinateurs et utilisateurs du réseau peuvent également accéder aux données que vous partagez (selon le paramétrage).

- **Autoriser ou bloquer les services de domaines** : un domaine est une sorte de répertoire de classification pour ordinateurs dans un réseau permettant une gestion centralisée des ordinateurs connectés au réseau. Il est généralement conseillé d'interdire les services de domaines dans les réseaux sensibles.

- **Utilisation partagée de la connexion Internet** : dans le cas de connexions directes à Internet, vous pouvez déterminer ici si tous les ordinateurs reliés au réseau par un ordinateur connecté à Internet peuvent accéder à Internet ou non. Ce partage de connexion Internet peut généralement être activé pour un réseau domestique.

- **Autoriser ou bloquer les services de réseau privé virtuel** : un réseau privé virtuel (ou VPN, Virtual Private Network) fait référence à la possibilité de connecter des ordinateurs ensemble et de créer ainsi une connexion directe entre eux. Pour que les services de réseau privé virtuel fonctionnent, ils doivent être autorisés par le pare-feu.

- **Éditeur de règles complet (mode expert)** : vous pouvez passer de l'assistant de règles au mode de modification avancé. Pour plus d'informations au sujet du mode de modification avancé, reportez-vous au chapitre **Utilisation du mode de modification avancé**.

Utilisation du mode de modification avancé

Si vous possédez certaines connaissances dans le domaine de la sécurité réseau, le mode de modification avancé vous permet de définir des règles personnalisées pour les différents réseaux. Vous pouvez y créer les mêmes règles que dans l'assistant des règles et définir des paramètres supplémentaires.

Les possibilités de réglage suivantes sont à votre disposition :

- **Nom** : Vous pouvez modifier le nom du jeu de règles sélectionné. L'ensemble de règles s'affiche ensuite sous ce nom dans la liste de la rubrique Ensembles de règleset peut être combiné aux réseaux identifiés par le pare-feu.
- **Mode furtif** : En mode furtif (caché, secret), les requêtes adressées à l'ordinateur dans le but de contrôler l'accessibilité de ses ports sont ignorées. Il est ainsi plus difficile pour les hackers de recueillir des informations sur le système.
- **Action si aucune règle ne s'applique** : vous pouvez indiquer ici si l'accès au réseau est généralement autorisé, refusé ou déterminé après un message de confirmation. Si des fonctions spéciales sont définies dans le cadre de la fonction d'apprentissage du pare-feu, celles-ci sont évidemment prises en compte.
- **Mode adaptatif** : le mode adaptatif prend en charge les applications employant la technique du canal retour (FTP et de nombreux jeux en ligne, par exemple). Les applications de ce type se connectent à un ordinateur distant et établissent avec ce dernier un canal retour par l'intermédiaire duquel l'ordinateur distant *se connecte à son tour* à votre application. Si le mode adaptatif est activé, le pare-feu reconnaît cette voie de retour et l'autorise sans vous en avertir.

Règles

La liste des règles regroupe toutes les règles définies pour le jeu de règles en cours. Vous pouvez ainsi autoriser l'accès au réseau à certains programmes, bien que le réseau ait été défini comme non fiable. Les règles figurant sur cette liste peuvent avoir été créées de différentes manières :

- à l'aide de **Assistant de règles**
- Directement à l'aide de la **mode de modification avancé**À l'aide du bouton **Nouveau**
- À partir de la boîte de dialogue de la boîte d'informations, qui s'affiche en cas d'**Alarme pare-feu** .

Chaque jeu de règles possède bien sûr sa propre liste de règles.

Les règles du pare-feu étant en partie organisées hiérarchiquement, il peut être important de vérifier leur ordre. Par exemple, un port autorisé pourrait être bloqué à nouveau par l'interdiction d'un accès protocole. Pour modifier la position d'une règle dans la liste, sélectionnez-la, puis déplacez-la dans la liste à l'aide des flèches de direction de la rubrique **Position**.

Lorsque vous créez une règle en mode de modification avancé ou modifiez une règle existante via la boîte de dialogue **Modifier**, le programme affiche la boîte de dialogue **Modifier la règle**, qui propose les paramètres suivants :

- **Nom** : c'est le nom du programme auquel s'applique la règle pour les règles prédéfinies et générées automatiquement.
- **Règle active** : si vous décochez cette case, la règle sera désactivée sans être supprimée.
- **Commentaire** : indique la manière dont la règle a été créée. Pour les règles prédéfinies du jeu de règles, l'entrée est Règle prédéfinie ; pour les règles créées dans la boîte de dialogue affichée en cas d'**Alarme pare-feu** , l'entrée est générée après avertissement ; pour les règles que vous avez créées en mode de modification avancé, vous pouvez saisir le commentaire de votre choix.
- **Sens de connexion** : détermine si la règle s'applique aux connexions entrantes et/ou sortantes.
- **Accès** : indique si l'accès doit être autorisé ou refusé pour le programme concerné par ce jeu de règles.
- **Protocole** : vous pouvez choisir les protocoles de connexion auxquels vous autorisez ou refusez l'accès. Il est possible de bloquer ou d'autoriser les protocoles de façon permanente ou de coupler l'utilisation du protocole à l'utilisation d'une ou de plusieurs applications en particulier (**Attribuer des applications**). Vous pouvez de la même manière définir les ports autorisés ou interdits à l'aide du bouton **Attribuer le service Internet**.
- **Période de temps** : vous pouvez également définir une plage horaire pendant laquelle l'accès aux ressources réseau est autorisé, par ex. n'autoriser l'accès que pendant vos heures de travail et l'interdire en dehors de celles-ci.
- **Plage d'adresses IP** : pour les réseaux avec adresses IP fixes, il est utile de réglementer leur utilisation en limitant la plage d'adresses IP autorisée. Une plage d'adresses IP clairement définie réduit nettement le risque d'intrusion.

Sauvegarde

Avec la numérisation croissante de notre vie quotidienne, l'utilisation de services de musique en ligne, les appareils photo numériques et la correspondance électronique, la sécurisation des données personnelles représente un enjeu de plus en plus important. Que ce soit en raison d'erreurs matérielles, de mégardes possibles ou de dommages causés par des virus ou des attaques de pirates, il faut régulièrement sécuriser vos documents personnels. Le logiciel G DATA effectue cette opération à votre place et protège ainsi vos documents et vos fichiers les plus importants, sans que vous ayez à vous en préoccuper.

Sauvegarder et rétablir

En cas de commande de sauvegarde via la fonction **Nouvelle commande**, vous pouvez utiliser les icônes suivantes :

Restauration : cette option permet de restaurer les données archivées dans la sauvegarde sur le système. Le déroulement de la restauration est détaillé au chapitre Restaurer la sauvegarde .

Sauvegarde : cette option vous permet de lancer la procédure de sauvegarde pour la commande définie immédiatement et en dehors de la série, indépendamment du programme prédéfini pour la sauvegarde.

Paramètres : vous pouvez modifier ici les paramètres pour la commande de sauvegarde que vous avez indiqués lors de la création de la commande de sauvegarde sous Nouvelle commande de sauvegarde .

Protocole : vous disposez ici d'une vue d'ensemble de tous les processus effectués dans le cadre de la commande de sauvegarde. Vous trouverez des entrées relatives aux processus de sauvegarde manuelle ou programmée effectués, des informations au sujet des éventuelles restaurations et, le cas échéant, des messages d'erreur (si le répertoire cible ne disposait pas de suffisamment d'espace mémoire pour la sauvegarde à exécuter, par exemple).

Nouvelle commande de sauvegarde



Pour créer une commande de sauvegarde, il vous suffit de cliquer sur le bouton **Nouvelle commande**.

Sélection des fichiers/disques durs/partitions

L'assistant de sauvegarde vous demande maintenant le type de sauvegarde que vous souhaitez exécuter.



Sauvegarde du fichier : il s'agit de la sauvegarde de certains fichiers ou dossiers dans un fichier d'archive.

Il vous suffit de sélectionner, dans les répertoires, les fichiers et les dossiers que vous souhaitez enregistrer. Nous vous recommandons d'enregistrer vos fichiers personnels lors d'une sauvegarde de fichiers et de ne pas sauvegarder les fichiers de programmes installés. Dans l'arborescence des répertoires, vous pouvez sélectionner et ouvrir des répertoires, dont le contenu sera ensuite affiché dans l'affichage des fichiers, en cliquant sur l'icône Plus. Tous les répertoires et fichiers dont la case à cocher est activée sont utilisés par le logiciel pour la sauvegarde. Si vous ne sélectionnez pas tous les fichiers et dossiers d'un répertoire pour la sauvegarde, le répertoire est signalé par une coche grisée.



Sauvegarde des lecteurs : il s'agit ici d'une sauvegarde complète des disques durs ou des partitions dans un fichier d'archive.

Sélection de la cible

Vous pouvez sélectionner ici la destination, donc l'emplacement où le logiciel G DATA doit créer la copie de sauvegarde des fichiers et des dossiers ou des disques durs et des partitions. Cela peut être un lecteur de CD ou de DVD-ROM, un autre disque dur, une clé USB, d'autres supports amovibles ou un répertoire réseau.

Nom de l'archive : vous pouvez définir ici un nom évocateur pour le fichier d'archive à créer comme, par exemple, *Fichiers de la sauvegarde hebdomadaire*, *Sauvegarde MP3*, etc.

Nouveau dossier : si vous souhaitez créer un nouveau dossier pour la sauvegarde, sélectionnez dans les répertoires l'emplacement d'enregistrement souhaité, puis cliquez sur le bouton **Nouveau dossier**.

> **Remarque** : nous attirons votre attention sur le fait que la sauvegarde ne doit pas être effectuée sur le même disque dur que celui sur lequel se trouvent les données d'origine. faute de quoi, en cas d'anomalie du disque en question, les données originales et les données de sauvegarde seraient perdues. L'idéal est de conserver une sauvegarde à un endroit différent de celui où se trouvent

les fichiers originaux (dans une autre pièce, sur un disque dur USB, sur un serveur FTP en réseau ou sur un CD/DVD-ROM, par exemple).

Créer une archive sur le serveur FTP : si vous avez accès à un serveur FTP, vous pouvez également effectuer votre sauvegarde en ligne sur ce serveur FTP. Il vous suffit de vous connecter avec les données d’accès au serveur FTP, votre archive de sauvegarde est ensuite reliée à votre serveur FTP. Vous pouvez également gérer les archives de sauvegarde via le **Navigateur FTP** intégré à votre logiciel G DATA.

Créer une archive dans le nuage : utilisez les services dans le nuage les plus courants, tels que Microsoft Dropbox, OneDrive ou Google Drive, pour créer une sauvegarde dans le nuage. Il vous suffit de vous connecter avec les données d’accès au service dans le nuage, votre archive de sauvegarde est ensuite reliée au nuage.

Remarque : lors des sauvegardes dans le nuage, vous devez veiller à ce que vos données de sauvegarde soient chiffrées. Dans la zone**Options** sous **Nouvelle commande de sauvegarde** vous pouvez activer ou désactiver le chiffrement des données.

Planning horaire

Vous pouvez indiquer ici la fréquence à laquelle vous souhaitez procéder à une sauvegarde des données sélectionnées et le type de sauvegarde qui doit être effectué. Il existe la sauvegarde complète au cours de laquelle toutes les données sélectionnées sont sauvegardées, mais également les sauvegardes partielles lors desquelles seules les modifications apportées depuis la dernière sauvegarde sont enregistrées.

Si vous sélectionnez l’option **Manuellement**, la sauvegarde n’est pas exécutée automatiquement. Vous devez la lancer via l’interface du programme. Sous l’option **Tous les jours**, vous pouvez indiquer, en saisissant les jours de la semaine, si l’ordinateur doit procéder au réglage uniquement les jours de la semaine, tous les deux jours ou le week-end, lorsque vous ne travaillez pas. Vous pouvez également définir des sauvegardes hebdomadaires et mensuelles.

Ne pas exécuter en mode batterie : vous pouvez indiquer que les sauvegardes ne doivent être exécutées que lorsque l’ordinateur portable est raccordé au réseau électrique de manière à ce que les sauvegardes ne soient pas interrompues parce que la batterie de l’ordinateur portable est déchargée.

Exécuter une sauvegarde complète

Il vous suffit d’indiquer, sous **Exécuter une sauvegarde complète**, la fréquence, les jours et les heures d’exécution de la sauvegarde. À la fréquence indiquée, le programme réalise une sauvegarde de l’ensemble des données que vous avez sélectionnées sous **Sélection des fichiers/disques durs/partitions** .

Attention : la sauvegarde programmée ne peut être exécutée sur un CD-ROM ou un DVD-ROM. Le changement de support nécessite en effet une intervention de l’utilisateur.

La rubrique **Suppression des anciennes archives** vous permet de définir comment le logiciel G DATA doit traiter les sauvegardes existantes. Le logiciel G DATA archive les données dans un fichier disposant de l’extension ARC. Les sauvegardes existantes, qui ne sont pas écrasées, contribuent bien évidemment à accroître la sécurisation de vos données, car même dans le cas où l'archive actuelle serait endommagée, les anciennes archives seraient toujours disponibles et donc tous les fichiers ne seraient pas perdus. Mais en règle générale, les archives nécessitent beaucoup de place sur les supports de données et vous devez donc veiller à ce que ne s'accumulent pas trop de fichiers d'archives. Il est recommandé d’indiquer, sous Conserver sauvegardes complètes, le nombre maximal de sauvegardes qui doivent être enregistrées sur le support de sauvegarde. L'archive la plus ancienne sera ensuite remplacée par l'archive actuelle.

Si vous activez la case à cocher **Créer des sauvegardes partielles**, le logiciel ne procède, une fois la première sauvegarde complète effectuée, qu’à des sauvegardes partielles, ce qui accélère la sauvegarde. Le processus peut cependant durer plus longtemps en cas de restauration d’une sauvegarde complète. Autre désavantage : la sauvegarde partielle nécessite davantage d’espace mémoire, les données de la sauvegarde complète devenues superflues n’étant pas directement supprimées. Après la prochaine sauvegarde complète les données de la sauvegarde complète et de la sauvegarde partielle sont par contre à nouveau réunies et la quantité de données est à nouveau identique à celle d'une sauvegarde complète.

Exécuter une sauvegarde partielle

Les sauvegardes partielles permettent d'accélérer la sauvegarde des données. Au lieu d’utiliser toutes les données pour la sauvegarde, la sauvegarde partielle se base sur une sauvegarde complète déjà existante et ne sauvegarde que les données qui ont été modifiées ou créées depuis la dernière sauvegarde complète. Vous disposez ainsi d’une sauvegarde complète de vos données, la procédure de sauvegarde est cependant nettement plus rapide.

Différentiel/Incrémentiel : lors de la sauvegarde différentielle, toutes les données modifiées ou ajoutées depuis la dernière sauvegarde complète sont enregistrées. La sauvegarde vient toujours compléter la dernière sauvegarde complète. Cette sauvegarde exige moins de temps et d’espace mémoire qu’une sauvegarde complète. La sauvegarde incrémentielle va également plus loin et enregistre, entre deux sauvegardes partielles, les fichiers modifiés depuis la dernière sauvegarde partielle. L’inconvénient étant toutefois qu’en cas de

restauration des données, vous avez besoin de plusieurs archives.

Options

La rubrique Options vous permet de modifier les options de sauvegarde générales. Vous n’avez généralement aucune modification à apporter ici, les options standard du logiciel G DATA couvrent en effet la plupart des cas.

Options d'archive générales

Dans les options d'archive générales, vous avez les possibilités suivantes de paramétrage :

- **Limiter la taille des fichiers de l'archive** : si vous enregistrez des archives sur CD-ROM, DVD-ROM ou autres CD vierges, il est important que le logiciel G DATA limite la taille des fichiers d’archive. Vous avez ici un choix de tailles par défaut, qui vous permet l'enregistrement ultérieur de données d'archives sur CD, DVD ou disques Blu-ray. L’archive se fractionne à l’approche de la taille maximale indiquée ici et les informations de sauvegarde sont réparties dans deux ou plusieurs fichiers d’archive.

- **Créer un CD/DVD à sessions multiples** : cette option permet de créer des CD ou DVD de sauvegarde réinscriptibles. Les contenus précédemment enregistrés ne sont pas supprimés, ils sont seulement complétés par les nouveaux contenus.

- **Supprimer les archives temporaires** : ce paramètre devrait être habituellement activé. Les archives temporaires ont besoin de beaucoup d'espace sur le disque dur après un certain nombre d'opérations de sauvegarde et ne sont en fait plus utilisées après leur utilisation temporaire.

- **Copier les fichiers du programme de récupération** : si vous activez cette fonction, un programme, grâce auquel vous pouvez restaurer vos données même si aucun logiciel G DATA n’est installé, est exécuté parallèlement aux données d’archive à l’emplacement d’enregistrement de la sauvegarde des données. Pour ce faire, démarrez le programme *AVKBackup* ou *AVKBackup.exe* à partir du CD/DVD-ROM.

  Le programme de restauration est uniquement copié sur CD/DVD-ROM. En cas de copies de sécurité sur des supports amovibles (clés USB, disques durs externes), cela n’est pas le cas.

  Si vous avez installé le logiciel G DATA sur l’ordinateur où doit s’effectuer la restauration, n’effectuez pas la restauration à l’aide du programme de restauration du CD/DVD-ROM, mais à l’aide de la fonction **Importer une archive**.

- **Rechercher d'éventuels virus avant l'archivage des fichiers** : si le module antivirus est installé, vous pouvez faire une recherche de virus dans vos données avant que celles-ci ne soient enregistrées dans l'archive de sauvegardes.

- **Vérifier l'archive après sa création** : cette fonction sert à vérifier la complétude et le bon état de l'archive après sa création.

- **Crypter l'archive** : si vous souhaitez protéger vos fichiers archivés d’un accès extérieur, vous pouvez les doter d’un mot de passe. Une restauration de données ne peut alors s'effectuer qu'avec ce mot de passe. Vous devriez retenir soigneusement ce mot de passe ou le noter dans un endroit sûr. Vous ne pouvez en effet pas restaurer vos données d’archive sans ce mot de passe.

- **Test d'intégrité lors d'une sauvegarde différentielle** : cette fonction permet de vérifier que la sauvegarde partielle créée est complète et ne présente pas d’erreurs.

- **Test d’intégrité lors de la restauration du disque dur** : cette fonction permet de vérifier le fonctionnement correct des données après la restauration. le **répertoire pour les fichiers temporaires** est le lieu d’enregistrement des données enregistrées sur le disque dur par le logiciel G DATA de manière temporaire uniquement. S'il ne restait pas suffisamment de place sur votre partition par défaut, vous pouvez changer ici la partition et l'espace de stockage temporaire de ces fichiers.

- **Utiliser la copie fantôme de Windows** : si cette option est désactivée, vous ne pouvez créer aucune image de la partition du système lors du fonctionnement.

Informations de l'utilisateur

pour pouvoir exécuter des sauvegardes programmées, vous devez activer la case à cocher, sous **Exécuter une tâche en tant que**, et saisir les données d’accès de votre compte utilisateur Windows. Ces informations sont nécessaires pour exécuter la sauvegarde à fréquence déterminée lorsque vous n'êtes pas connecté en tant qu'utilisateur.

Compression

Vous pouvez déterminer si vos archives sont fortement ou faiblement compressées dans la rubrique Compression.

- **Bonne compression** : Les données sont fortement compressées en vue de la sauvegarde. Vous épargnez ce faisant de l'espace mémoire, mais la sauvegarde dure cependant plus longtemps.

- **Compression uniforme** : La sauvegarde n'est pas si intensément compressée, mais elle dure par contre moins longtemps.
- **Exécution rapide** : Aucune compression de données, la sauvegarde s'effectue en revanche rapidement.

Exclure des fichiers

Le logiciel G DATA se base généralement sur le format des fichiers pour la sauvegarde. Votre système comporte des formats correspondants mais également certains domaines administrés automatiquement et dont la sauvegarde est inutile, car leurs fichiers ne sont que temporaires (s'ils servent par exemple à la représentation plus rapide des pages web.) Pour que le logiciel G DATA n’archive pas ces fichiers inutilement, vous pouvez désactiver la case à cocher.

- **Dossier temporaire avec fichiers** : si cette option est activée, les dossiers temporaires, ainsi que leurs fichiers et sous-dossiers, ne seront pas inclus dans la procédure de sauvegarde.
- **Répertoires Internet temporaires avec des fichiers** : si cette option est activée, les dossiers d’enregistrement de sites Internet, ainsi que leurs fichiers et sous-dossiers ne seront pas inclus dans la procédure de sauvegarde.
- **Thumbs.db** : l’activation de cette option exclut de la sauvegarde les fichiers thumbs.db créés automatiquement par Windows Explorer. Ces fichiers servent par exemple à gérer l'affichage des miniatures de diaporama. Ils sont automatiquement créés à partir des images d'origine.
- **Fichiers temporaires (attribut de fichier)** : l’activation de cette option exclut de la sauvegarde les fichiers que votre système a définis comme temporaires.
- **Fichiers système (attribut de fichier)** : l’activation de cette option exclut de la sauvegarde les fichiers que votre système a définis comme étant des fichiers système.
- **Exclure les types de fichiers** : cette fonction vous permet de définir vous-même les extensions de fichiers que la sauvegarde ne doit pas prendre en compte. Procédez comme suit : sous **Type de fichiers (par ex. *.txt)**, saisissez l’extension ou le nom de fichier que vous souhaitez exclure. Cliquez ensuite sur **OK**. Répétez la procédure pour tous les autres types et noms de fichiers que vous souhaitez exclure (par exemple, picasa.ini, *.ini, *bak, etc.). Vous pouvez utiliser ici l’icône en forme d’astérisque et l’icône en forme de point d’interrogation comme caractères génériques.

  Les caractères de remplacement fonctionnent comme suit :

  L’icône en forme de point d’interrogation (?) représente des caractères uniques.

  L’astérisque (*) remplace des suites de caractères.

  Par exemple, pour vérifier l’intégralité des fichiers comportant l’extension de fichier exe, vous devez saisir *.exe. Pour désigner des fichiers de feuilles de calcul de différents formats (*.xlr, *.xls, etc.), il vous suffit de saisir *.xl?. Pour désigner des fichiers de types différents mais dont le début du nom est identique, saisissez par exemple texte*.*.

Appliquer les options par défaut actuelles

Cliquez sur ce bouton pour rétablir les paramètres par défaut définis pour le logiciel G DATA. Si, lors de la création de sauvegardes, vous avez défini par mégarde des instructions invalides concernant les paramètres et ne savez pas comment les rectifier, cliquez sur le bouton **Appliquer les options par défaut actuelles**.

Restaurer la sauvegarde



Vous pouvez restaurer ici les fichiers d’origine enregistrés dans le cadre d’une sauvegarde après une perte de données. Pour ce faire, il vous suffit de cliquer sur le bouton **Restaurer**.

Une boîte de dialogue, dans laquelle toutes les procédures enregistrées pour la commande de sauvegarde sont exécutées, s’affiche.

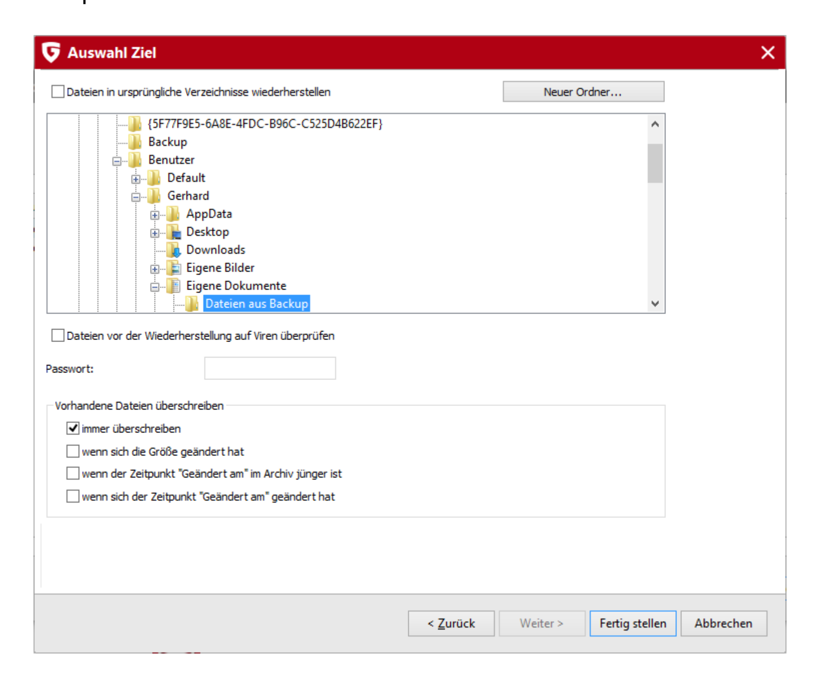
Sélectionnez ici la sauvegarde souhaitée (dernière sauvegarde effectuée, si vous souhaitez restaurer des documents supprimés par inadvertance peu de temps avant, par exemple), puis cliquez sur le bouton **Restaurer**.

Vous avez maintenant la possibilité de définir la forme de restauration souhaitée :

- **Restaurer la sauvegarde complète** : tous les fichiers et dossiers enregistrés à l’aide de cette sauvegarde sont restaurés.
- **Restaurer uniquement des partitions/des fichiers sélectionnés** : le répertoire de sauvegarde, dans lequel vous pouvez sélectionner de manière ciblée les fichiers, dossiers ou partitions que vous souhaitez restaurer, s’affiche. Dans l’arborescence des répertoires, vous pouvez sélectionner et ouvrir des répertoires, dont le contenu sera ensuite affiché dans l’affichage des fichiers, en cliquant sur

l'icône Plus. Tous les répertoires et fichiers dont la case à cocher est activée sont restaurés à partir de la sauvegarde. Les dossiers, dont certains des fichiers ne doivent pas être analysés, sont signalés par une coche grisée.

Vous pouvez ensuite indiquer si les fichiers doivent être ou non restaurés dans leurs répertoires d'origine. Si les fichiers sont enregistrés à un autre emplacement, vous pouvez éventuellement sélectionner, sous **Nouveau dossier**, le dossier dans lequel les fichiers doivent être placés. Saisissez, sous **Mot de passe**, le mot de passe d'accès, au cas où vous avez compressé votre sauvegarde en la protégeant à l'aide d'un mot de passe.



Lorsque vous restaurez les fichiers dans leurs répertoires d'origine, vous disposez des options suivantes pour ne rétablir que les fichiers modifiés :

- **Toujours remplacer** : Avec ce paramètre, on accorde aux fichiers issus de la sauvegarde de données plus d'importance qu'aux données se trouvant dans le répertoire d'origine. Si vous deviez cocher cette case, les données éventuellement encore présentes seraient écrasées par les données se trouvant dans l'archive.

- **Lorsque la taille de fichier est différente** : Avec ce paramètre, les données présentes dans le répertoire d'origine ne sont écrasées que si le fichier d'origine a été modifié. Les fichiers dont la taille n'a pas été modifiée sont ignorés. La restauration des données est ainsi plus rapide.

- **Lorsque le moment "Modifié le" est plus récent dans l'archive** : Ici, les fichiers du répertoire d'origine sont toujours remplacés par les copies de l'archive lorsqu'elles sont plus récentes. La restauration des données peut être ici aussi plus rapide, étant donné que seules les données modifiées sont restaurées.

- **Lorsque le moment "Modifié le" est différent** : Ici, les données du répertoire d'origine sont toujours remplacées lorsque la date de la modification des fichiers archivés a changé.

Cliquez ensuite sur le bouton **Terminer le processus** pour procéder à la restauration conformément aux paramètres définis.

Actions

Cette zone vous permet d'effectuer, entre autres, des actions pour la maintenance de vos sauvegardes de données.

Les programmes de services suivants sont à votre disposition :

Entretenir une archive en ligne

Si vous désirez sauvegarder vos données importantes en ligne, sur le serveur FTP de G DATA, le logiciel G DATA a bien évidemment besoin des données d'accès correspondantes. Vous pouvez saisir ici le nom du serveur, le port, le nom d'utilisateur, le mot de passe et le répertoire qui vous ont été communiqués lors de votre enregistrement sur le serveur de mise à jour G DATA.

Espace mémoire en ligne inclus (1 Go)

Lors de l'enregistrement du logiciel, G DATA met gratuitement à votre disposition un espace mémoire en ligne de 1 Go sur un serveur FTP pour vos sauvegardes. Les données FTP nécessaires sont automatiquement transmises dans le formulaire de saisie FTP du logiciel G DATA. Vous pouvez ainsi conserver vos données les plus importantes en ligne et les protéger à l'aide d'un mot de passe si nécessaire. Les

données d'accès FTP nécessaires vous sont communiquées dans un courrier électronique de confirmation, après enregistrement du logiciel.

Dans le cas de licences multipostes, vous disposez naturellement d'un espace mémoire de 1 Go pour chaque licence, par exemple trois fois 1 Go pour une licence trois postes.

Si vous êtes abonné aux mises à jour des signatures antivirus G DATA, vous disposez de cet espace mémoire FTP. Lorsque le contrat touche à sa fin, vous disposez encore d'une période de 30 jours pour supprimer vos données du serveur de sauvegarde G DATA. Les données sont ensuite détruites.

Navigateur FTP

Il vous suffit de saisir vos données d'accès FTP pour accéder à votre serveur FTP G DATA. Ces données vous ont été transmises par courrier électronique lors de l'enregistrement en ligne de votre produit. Vous pouvez effectuer les actions suivantes dans le navigateur FTP :

 **Se connecter** : Si la connexion au navigateur FTP devait être interrompue, vous pouvez la rétablir ici.

 **Se déconnecter** : Vous pouvez ici interrompre la connexion au navigateur FTP.

 **Nouveau dossier** : Si vous souhaitez enregistrer vos sauvegardes dans différents dossiers (uniquement des dossiers spéciaux réservés aux sauvegardes de musique, par exemple), vous pouvez créer un dossier sur votre espace FTP grâce à cette fonction.

 **Supprimer** : Cette fonction vous permet de supprimer des dossiers ou des archives qui ne sont plus nécessaires.

 **Actualiser** : si vous avez dû procéder à une mise à jour lors de l'utilisation du navigateur FTP, vous pouvez afficher les nouvelles données à l'aide du bouton Actualiser.

 **Téléchargement** : Vous pouvez ici copier à l'aide de la souris des archives sélectionnées du serveur FTP sur un espace de stockage de votre ordinateur.

 **Téléchargement en amont** : vous pouvez enregistrer les archives créées avec le logiciel G DATA sur votre serveur FTP.

 **Aide** : cette option vous permet d'afficher l'aide du programme.

Graver a posteriori des archives sur CD/DVD

Il est également possible de graver les fichiers de sauvegarde ultérieurement sur CD ou DVD. Il vous suffit pour cela de sélectionner le projet que vous souhaitez graver dans la boîte de dialogue qui apparaît et de cliquer sur le bouton **Suivant**.

Sélectionnez maintenant le lecteur sur lequel vous souhaitez graver la sauvegarde des données.

Les options suivantes sont ici à votre disposition :

- **Vérifier les données après le gravage** : Si vous cochez cette case, les données gravées seront vérifiées une nouvelle fois après la procédure de gravure. Cela dure un peu plus longtemps qu'une procédure de gravure sans vérification, mais cela est généralement recommandé.

- **Copier les fichiers du programme de récupération** : si vous activez cette fonction, un programme, grâce auquel vous pouvez restaurer vos données même si aucun logiciel G Data n'est installé, est exécuté parallèlement aux données d'archive à l'emplacement d'enregistrement de la sauvegarde des données. Pour ce faire, démarrez le programme *AVKBackup* ou *AVKBackup.exe* à partir du CD/DVD-ROM.

Cliquez sur le bouton **Graver** pour démarrer la procédure de gravure. Le CD/DVD est automatiquement éjecté après la procédure de gravure.

> **Remarque** : les données de sauvegarde ne sont bien évidemment pas supprimées du support de données d'origine après la procédure de gravure. La gravure ultérieure sur CD/DVD est une sécurité supplémentaire.

Importer une archive

Pour restaurer des archives et des sauvegardes de données qui ne se trouvent pas sur un lecteur géré par le logiciel G Data, utilisez la fonction **Importer une archive**. Une boîte de dialogue s'ouvre alors dans laquelle vous pouvez rechercher les fichiers d'archives souhaités, comportant l'extension *ARC*, sur un CD, un DVD ou un réseau, par exemple. Lorsque vous avez trouvé l'archive souhaitée, veuillez cocher sa case et cliquer ensuite sur le bouton **OK**. Une fenêtre d'information vous informe que l'archive a été importée avec succès. Si vous désirez utiliser cette archive pour une restauration de données, il vous suffit de vous rendre dans la zone **Restaurer** du logiciel G Data, de sélectionner la sauvegarde souhaitée et de démarrer la restauration.

Remarque : les fichiers d'archive créés par le logiciel G Data présentent l'extension ARC.

Copier le disque dur

Le clonage d'un disque dur permet non seulement de copier les données sur un autre support mais également de transférer l'intégralité du contenu du disque dur, bit par bit. Vous pouvez ainsi remplacer un disque dur système ou l'échanger contre un plus grand sans devoir réinstaller l'ensemble du système d'exploitation et des programmes. Si nécessaire, une copie complète de votre ordinateur est également à votre disposition.

Attention : le disque dur sur lequel vous procédez au clonage doit disposer d'au moins la même capacité de stockage que le disque dur d'origine.

- Étape 1 : sélectionnez la source (le disque dur) que vous souhaitez copier.
- Étape 2 : sélectionnez maintenant la destination (le disque dur sur lequel le clone du disque dur d'origine doit être créé).

Si vous activez la case à cocher **Modifier la taille des partitions en fonction de la taille du disque dur cible**, les partitions sont agrandies en fonction er leur taille actuelle et ajustées ainsi à des lecteurs de sauvegarde de plus grande taille. Si le disque d'origine et le disque de sauvegarde ont la même taille, les partitions conservent leur taille d'origine.

Créer un support d'amorçage

Pour restaurer des sauvegardes, vous pouvez créer un CD/DVD ou une clé USB contenant un logiciel spécifique, qui vous permet de procéder à la restauration des données, même si aucun logiciel G Data n'est installé. Pour restaurer des sauvegardes de cette manière, lancez le support d'amorçage et sélectionnez le programme *AVKBackup* ou le fichier *AVKBackup.exe*. Vous pouvez alors sélectionner les sauvegardes souhaitées et lancer la restauration.

Remarque : la procédure de création d'un support d'amorçage est détaillée au chapitre **Support d'amorçage** suivant. Le support d'amorçage a deux fonctions pour les logiciels G Data. Il permet de procéder à la restauration de sauvegardes et de vous assurer de l'absence de virus sur votre ordinateur avant le démarrage de Windows (avec l'aide de l'analyse BootScan).

Tuner

Qu'il s'agisse de rappels automatiques de mises à jour Windows, de défragmentations programmées à fréquence régulière, du nettoyage régulier des entrées caduques du registre et des fichiers temporaires, le tuner vous offre un outil d'accélération et de simplification de votre système Windows.

Vous pouvez configurer votre ordinateur manuellement, à l'aide de boutons, ou procéder à des réglages réguliers, programmés dans le temps.



Dernière optimisation : ce champ indique quand le réglage de l'ordinateur a été effectué pour la dernière fois. Pour procéder à un nouveau réglage, sélectionnez l'entrée **Procéder maintenant au réglage** d'un clic. Dès le réglage lancé, une barre de progression vous indique l'évolution du réglage.



Optimisation automatique : si vous souhaitez automatiser le réglage de votre ordinateur, vous pouvez créer un réglage programmé en cliquant sur l'entrée **Activer l'optimisation automatique**. Pour paramétrer le réglage automatique, sélectionnez l'option **Autres paramètres**.



Configuration : cette **rubrique** vous permet de sélectionner tous les modules que le tuner doit utiliser lors des réglages. Les modules sélectionnés sont à cette occasion soit démarrés par une action automatique à fréquence déterminée (voir chapitre **Planification**) soit par une action manuelle. Un double-clic sur un module vous permettra de l'activer. Vous pouvez optimiser chacune des grandes rubriques de réglage suivantes :

- *Sécurité* : différentes fonctions qui téléchargent automatiquement des données à partir d'Internet, ne concernent que le fournisseur. Souvent, ces fonctions laissent entrer des logiciels nuisibles (malware). Grâce à ces modules, votre système est protégé et actualisé au maximum.
- *Performance* : les fichiers temporaires comme les copies de sécurité, les protocoles et les données d'installation qui occupent de l'espace de stockage mais ne sont plus utilisés après installation peuvent ralentir votre disque dur. De plus, ils occupent un espace de stockage non négligeable. Les processus et les icones de fichiers qui ne sont plus utilisés peuvent par ailleurs notoirement ralentir votre système. Les modules répertoriés ici vous permettront de libérer votre ordinateur de ces éléments encombrants superflus et d'accélérer ses performances.
- *Protection des données* : les modules qui se chargent de la protection de vos données sont regroupés ici. Les traces indésirables provenant de votre parcours sur Internet ou du mode d'utilisation de votre ordinateur qui peuvent trahir des informations sensibles et des mots de passe importants peuvent être effacées ici.



Restauration : le logiciel crée un point de restauration pour chaque modification effectuée. Si un des réglages venait à provoquer des résultats indésirables, vous pouvez l'annuler en restaurant le système. Veuillez également lire à ce propos le chapitre **Restauration**.

Restauration

le logiciel crée un point de restauration pour chaque modification effectuée. Si un des réglages venait à provoquer des résultats indésirables, vous pouvez l'annuler en restaurant le système.



Tout sélectionner : si vous souhaitez refuser toutes les modifications apportées dans le cadre du réglage, sélectionnez tous les points de restauration et cliquez sur le bouton **Restaurer**.



Restauration : si vous souhaitez ne refuser que certaines des modifications apportées dans le cadre du réglage, sélectionnez le point de restauration souhaité et cliquez sur le bouton **Restaurer**.



Supprimer les éléments sélectionnés : ce bouton vous permet de supprimer les points de restauration dont vous n'avez plus besoin.

Contrôle parental

Le contrôle parental vous permet de réguler l'utilisation d'Internet et de l'ordinateur par vos enfants.

Sous **Utilisateur**, sélectionnez un des utilisateurs connectés sur l'ordinateur et définissez ensuite les limitations correspondantes. Les boutons **Nouvel utilisateur...** vous permet de créer des comptes sur votre ordinateur (pour vos enfants, par exemple).

- **Contrôle parental pour cet utilisateur** : vous pouvez activer ou désactiver ici le contrôle parental pour l'utilisateur sélectionné.
- **Contenu non autorisé** : dans cette rubrique s'ouvre une boîte de dialogue vous permettant de bloquer des contenus Web pour l'utilisateur affiché. Cliquez sur **Modifier** pour définir les contenus interdits pour l'utilisateur sélectionné.
- **Contenu autorisé** : cette rubrique affiche une boîte de dialogue dans laquelle vous pouvez autoriser des contenus Web pour l'utilisateur affiché. Cliquez sur **Modifier** pour définir les contenus autorisés pour l'utilisateur sélectionné.
- **Surveillance du temps d'utilisation d'Internet** : vous pouvez indiquer ici la durée et les horaires d'accès à Internet pour l'utilisateur sélectionné. Cliquez sur **Modifier** pour définir les temps d'utilisation pour l'utilisateur sélectionné.
- **Surveillance du temps d'utilisation de l'ordinateur** : vous pouvez indiquer ici la durée et les heures d'utilisation de l'ordinateur par l'utilisateur sélectionné. Cliquez sur **Modifier** pour définir les temps d'utilisation pour l'utilisateur sélectionné.

Paramètres : vous permet de modifier et de personnaliser les principaux paramètres du contrôle parental.

Créer un utilisateur

Cliquez sur le bouton **Nouvel utilisateur**. Le programme affiche une boîte de dialogue dans laquelle vous pouvez saisir le nom du nouvel utilisateur et son mot de passe.

> **Remarque** : pour plus de sécurité, il est conseillé de choisir un mot de passe de huit caractères au moins, associant majuscules, minuscules et chiffres.

Le nom d'utilisateur nouvellement créé apparaît désormais sous **Utilisateur**, un compte utilisateur Windows a été simultanément créé pour cet utilisateur. Cela signifie que le contrôle parental est automatiquement activé pour la personne se connectant avec ce nom d'utilisateur au démarrage de Windows. Double-cliquez maintenant sur la rubrique de paramètres qui doivent être définis pour cet utilisateur (par exemple, interdiction des contenus non autorisés ou mise à disposition exclusive des contenus autorisés) ou déterminez s'il faut surveiller Temps d'utilisation d'Internet ou durée d'utilisation de l'ordinateur de cet utilisateur.

Contenu non autorisé

Dans cette rubrique s'ouvre une boîte de dialogue vous permettant de bloquer les contenus Web de votre choix pour l'utilisateur sélectionné. Sélectionnez à cet effet les catégories dont vous voulez interdire l'accès en cochant les cases correspondantes. Cliquez ensuite sur **OK** pour bloquer les sites Internet répondant aux critères définis.

Cliquez sur le bouton **Nouveau** pour ouvrir une boîte de dialogue et définir vos critères de blocage (également appelés listes noires). Donnez d'abord un nom, puis attribuez le cas échéant des informations au filtre créé individuellement.

Cliquez sur **OK**. Le programme affiche une autre boîte de dialogue dans laquelle vous devez indiquer les contenus que le filtre doit bloquer.

Pour ce faire, saisissez, sous **Filtre**, le terme à bloquer et, sous **Lieu de la recherche**, la zone du site Web où le terme indiqué doit être recherché.

Les options suivantes sont disponibles :

- **Adresse URL** : si vous activez cette case à cocher, le texte à bloquer est recherché dans l'adresse Web. Si, par exemple, vous voulez interdire les sites *www.chatcity.no*, *www.crazychat.co.uk*, etc., saisissez *chat* sous **Filtre**, activez la case à cocher **URL** et cliquez sur le bouton **Ajouter**. Tous les sites dont le nom de domaine (adresse Internet) contient le mot *chat* seront ainsi bloqués.
- **Titre** : validez l'option «URL» pour rechercher le texte à bloquer dans le titre de l'adresse Web. Il s'agit du texte qui apparaît quand vous ajoutez une page à vos favoris. Si, par exemple, vous voulez interdire les sites *Chat City Detroit*, *Teenage Chat 2005*, etc., saisissez *chat* sous **Filtre**, activez la case à cocher **Titre** et cliquez sur le bouton **Ajouter**. Tous les sites dont le titre contient le mot *chat* seront ainsi bloqués.
- **Meta** : les balises META sont des entrées de texte masquées sur les sites, servant au référencement dans les moteurs de recherche. Les termes tels que *sexe* ou *chat* sont souvent utilisés pour augmenter les accès aux sites. Si vous voulez interdire les sites dont les

métabalises contiennent le mot *chat*, saisissez *chat* sous **Filtre**, activez la case à cocher **Meta** et cliquez sur le bouton **Ajouter**. Tous les sites dont les balises Meta contiennent le mot *chat*seront ainsi bloqués.

- **Dans tout le texte** : si vous voulez que le programme examine les contenus à bloquer dans le contenu visible des sites Web, saisissez le terme voulu (*chat*, par exemple), activez la case à cocher **Dans tout le texte** et cliquez sur le bouton **Ajouter**. Tous les sites dont le texte affiché contient le mot *chat* seront ainsi bloqués.

la fonction Exceptions permet d'autoriser des sites qui tombent sous le coup d'un filtre. Il vous suffit de cliquer sur le bouton **Exceptions** et de saisir le site correspondant.

> **Remarque** : vous pouvez modifier ou supprimer les filtres que vous avez créés dans la rubrique Mes filtres. Consultez pour cela la rubrique **Mes filtres**.

Contenu autorisé

Cette rubrique affiche une boîte de dialogue dans laquelle vous pouvez autoriser à un utilisateur sélectionné des contenus Web spéciaux. Choisissez les catégories dont vous voulez autoriser l'accès en cochant les cases correspondantes. Cliquez ensuite sur **OK** pour que les sites répondant aux critères définis soient autorisés.

Cliquez sur le bouton **Nouveau** pour ouvrir une boîte de dialogue et définir les contenus autorisés (également appelés listes blanches). Donnez d'abord un nom, puis attribuez le cas échéant des informations au filtre créé individuellement.

Cliquez ensuite sur **OK**. Dans la boîte de dialogue suivante, vous pouvez ajouter à la liste blanche les sites de votre choix, par exemple les sites adaptés à un jeune public.

Saisissez sous **Filtre** les parties de noms de domaines à autoriser. Si, par exemple, vous souhaitez autoriser l'accès au site de la chaîne Disney Channel, saisissez *disneychannel*. Saisissez maintenant sous **Description** ce que contient ce site Web (dans le cas présent *Elefanti - site Web pour les enfants*) et saisissez sous **Lien vers offre** l'adresse Web exacte du site. La description ainsi que le lien jouent un rôle important lorsque votre enfant appelle une page non autorisée, par exemple. Au lieu d'un message d'erreur, le programme charge alors dans le navigateur une page HTML affichant la liste de tous les sites Internet compris dans la liste blanche, accompagnés de leur description. Votre enfant pourra ainsi consulter les pages dont l'accès lui a été autorisé. Après avoir défini tous les paramètres, cliquez sur le bouton **Ajouter** pour ajouter le site à la liste blanche.

> **Remarque** : le filtre recherche des segments dans les noms de domaines. Les résultats peuvent donc varier selon ce que vous avez saisi sous « Filtre ». Dans certains cas, il sera nécessaire de définir des restrictions plus sévères.

Surveillance du temps d'utilisation de l'Internet

Vous pouvez déterminer ici la durée et les horaires d'accès à Internet de l'utilisateur sélectionné. Pour ce faire, cochez la case **Surveillance du temps d'utilisation de l'Internet**. Vous pouvez alors définir pour l'utilisateur la durée totale de l'accès à Internet sur une base mensuelle, hebdomadaire et combien d'heures pour quels jours de la semaine. Vous pouvez, par exemple, autoriser un accès prolongé le week-end et plus réduit en semaine pour les enfants scolarisés. Pour ce faire, vous n'avez qu'à saisir les périodes horaires sous **Jour/hh:mm**. La saisie *04/20:05* représente, par exemple, une durée d'utilisation d'Internet de 4 jours, 20 heures et 5 minutes.

> **Remarque** : C'est toujours la plus petite valeur qui compte dans l'interaction des quotas d'utilisation Internet. Par exemple, si vous définissez une limite d'utilisation de quatre jours dans le mois mais autorisez cinq jours dans la semaine, le logiciel réglera automatiquement l'utilisation Internet de l'utilisateur sur quatre jours.

Si un utilisateur essaie d'accéder à Internet alors que son quota autorisé est dépassé, le navigateur affiche un avertissement l'informant du dépassement de quota.

Établir horaires de non-autorisation

Le bouton **Établir horaires de non autorisation** ouvre une boîte de dialogue dans laquelle vous pouvez définir des périodes horaires d'utilisation dans la semaine, en plus du quota horaire d'utilisation d'Internet. Les périodes bloquées sont représentées en rouge et les périodes autorisées en vert. Pour autoriser ou bloquer une période, il vous suffit de la sélectionner avec la souris. Un menu contextuel s'affiche alors près du pointeur de la souris et vous offre deux possibilités : **Débloquer du temps** et **bloquer du temps**. Lorsqu'un utilisateur essaie d'accéder à Internet durant une période bloquée, le navigateur affiche un écran l'avertissant que l'accès à Internet n'est pas autorisé à ce moment-là.

Surveillance de la durée d’utilisation de l’ordinateur

Vous pouvez déterminer ici la durée et les horaires d’utilisation de l’ordinateur par l’utilisateur sélectionné. Pour ce faire, cochez la case **Surveillance de la durée d'utilisation de l'ordinateur**. Vous pourrez ensuite déterminer la durée mensuelle ou hebdomadaire maximale d'accès à l'ordinateur d'un certain utilisateur et sa durée maximale d'utilisation chaque jour de la semaine. Vous pouvez, par exemple, autoriser un accès prolongé le week-end et plus réduit en semaine pour les enfants scolarisés. Pour ce faire, il vous suffit de saisir les périodes horaires sous **Jour/hh:mm**. La saisie *04/20:05* représente, par exemple, un temps d'utilisation de l'ordinateur de 4 jours, 20 heures et 5 minutes. Le bouton **Message d'avertissement avant la fin du temps autorisé** accorde à l'utilisateur le temps de sauvegarder ses travaux en cours, avant que son temps d'utilisation ne s'écoule. L'extinction sans avertissement de l'ordinateur peut provoquer des pertes de données.

> **Remarque** : Dans le cas d’une incohérence dans les paramètres d’utilisation de l’ordinateur, la valeur inférieure l’emporte. Ainsi, si vous avez défini une limite de 4 jours par mois, mais 5 jours par semaine, la limitation hebdomadaire sera automatiquement réduite à 4 jours.

Établir horaires de non-autorisation

Le bouton **Établir horaires de non autorisation** ouvre une boîte de dialogue dans laquelle vous pouvez définir des périodes horaires d'utilisation dans la semaine, en plus du quota horaire d'utilisation de l'ordinateur. Les périodes bloquées sont représentées en rouge et les périodes autorisées en vert. Pour autoriser ou bloquer une période, il vous suffit de la sélectionner avec la souris. Un menu contextuel s'affiche alors près du pointeur de la souris et vous offre deux possibilités : **Débloquer du temps** et **bloquer du temps**.

Mes filtres

Cette rubrique vous permet de modifier vos listes blanches (contenus autorisés) et vos listes noires (contenus interdits) et de créer manuellement de nouvelles listes.

On distingue en théorie les types de listes suivants :

- **Contenu autorisé** : si vous activez une liste blanche pour l'un des utilisateurs sélectionné ci-dessus, celui-ci peut consulter uniquement les sites Internet figurant sur cette liste. Vous pouvez, en tant qu’administrateur, modifier cette liste blanche à votre guise ou créer une liste pour un utilisateur à partir des listes blanches prédéfinies. Remarque : les listes blanches sont particulièrement indiquées pour octroyer aux jeunes enfants un accès très limité à Internet afin qu’ils puissent visiter seulement des sites à contenu pédagogique.

- **Contenu non autorisé** : la liste noire vous permet d'interdire à l'utilisateur sélectionné d'accéder aux sites qu'elle contient. Tout ce qui ne figure pas dans cette liste lui est librement accessible. Remarque : veuillez noter que cette fonction permet de bloquer l'accès à certaines pages mais n'empêche en rien l'utilisateur de consulter des contenus similaires sur d'autres sites. Les listes noires d'adresses Internet ne constituent donc pas une protection totale contre les contenus indésirables.

Les options suivantes vous permettent de modifier les listes d'exclusion :

- **Supprimer** : la fonction **Supprimer** vous permet de supprimer les listes sélectionnées à l’aide de la souris.

- **Nouveau** : vous permet de créer une liste noire ou blanche entièrement nouvelle. La procédure est la même que celle décrite à la rubrique **Contenu non autorisé** et **Contenu autorisé** .

- **Modifier** : modifier le contenu d'une liste existante.

Paramètres : protocole

Vous pouvez modifier ici les paramètres de base pour les informations de la rubrique Protocole. Ainsi, vous pouvez déterminer si des attaques contre des contenus autorisés et/ou interdits doivent ou non faire l'objet d'un journal. Si les contenus font l'objet d'un journal, vous pouvez voir les journaux des différents utilisateurs à la rubrique Journaux.

Comme les fichiers journaux deviennent de plus en plus lourds en cas d’utilisation régulière, vous pouvez vous faire rappeler par le contrôle parental, sous **Afficher un message si un fichier atteint ___ Ko**, que les fichiers journaux ont dépassé une certaine taille et que vous devez les supprimer manuellement dans la rubrique **Protocole**, sous **Supprimer le journal**.

Coffre de données

Le coffre de données protège les données sensibles à l'image d'un coffre à la banque. Il est possible d'installer un coffre en tant que lecteur supplémentaire ou que partition du disque dur, l'utilisation du coffre est donc très facile.

Vous disposez des possibilités suivantes pour créer et gérer des coffres :

- **Actualiser** : si vous avez ouvert ou fermé le coffre en dehors du module de coffres de données, nous vous recommandons de cliquer sur Actualiser pour mettre à jour l'affichage du statut des coffres gérés.
- **Ouvrir/Fermer** : vous pouvez ici ouvrir ou fermer les coffres qui se trouvent sur votre ordinateur et sur les supports connectés. Nous attirons votre attention sur le fait que, pour ouvrir un coffre, vous avez besoin du mot de passe que vous avez indiqué à la création du coffre. Les coffres peuvent ici être fermés sans mot de passe.
- **Créer un coffre** : cette fonction vous permet de créer un coffre. Un assistant qui vous aide à créer le coffre s'affiche. Consultez pour cela la rubrique Créer un coffre.
- **Créer un coffre-fort mobile** : dès qu'un coffre est créé, vous pouvez le convertir en coffre portable. Vous pouvez le configurer de manière à pouvoir l'utiliser sur une clé USB ou à l'envoyer par courrier électronique. Consultez pour cela la rubrique Créer un coffre-fort mobile.
- **Supprimer** : la gestion des coffres vous offre une vue d'ensemble de tous les coffres qui se trouvent sur votre ordinateur et sur les supports connectés. Vous pouvez supprimer ici les coffres dont vous n'avez plus besoin. Nous attirons votre attention sur le fait que vous pouvez également supprimer des coffres dont vous ne connaissez pas le mot de passe. Vous devez donc vérifier que vous n'avez vraiment plus besoin du contenu des coffres à supprimer.

Créer un coffre

Une boîte de dialogue interactive vous aide lors de la création de coffres. Cliquez sur le bouton **Suivant** pour poursuivre.

Emplacement d'enregistrement et taille du coffre-fort

Définissez maintenant l'emplacement d'enregistrement et la taille du coffre.

> **Remarque** : le coffre est un fichier protégé qui fonctionne comme une partition de disque dur lorsqu'il est ouvert. Vous pouvez créer un fichier de coffre à l'emplacement souhaité de votre disque dur. Vos données sont enregistrées dans le coffre sous un format chiffré. Une fois le coffre ouvert, vous pouvez traiter, supprimer, copier et déplacer les fichiers et les répertoires comme sur un disque dur ou une partition de disque dur classique.

Emplacement d'enregistrement

Sélectionnez ici le support de données (par exemple, support de données local (C:)) sur lequel le coffre doit être créé.

> **Remarque** : Les coffres créés dans un répertoire protégé ne sont visibles sur l'ordinateur que lorsque le logiciel G DATA est installé. Si vous désinstallez le logiciel, les coffres de données créés ne sont plus visibles.

Taille du coffre-fort

Sélectionnez ensuite une taille de coffre en positionnant le curseur de manière adaptée. Vous disposez d'autant d'espace que disponible au niveau de l'emplacement d'enregistrement. D'une manière générale, la taille maximale doit toutefois rester inférieure à 2 Go, afin que votre système ne soit pas ralenti par un manque d'espace mémoire.

> **Remarque** : Les boutons situés à gauche du curseur de taille du coffre vous permettent de procéder à une sélection rapide. Vous pouvez ainsi définir très précisément la taille du coffre ou adapter la taille du coffre à la taille autorisée pour la gravure sur un CD, un DVD ou un BluRay, par exemple.

Cliquez maintenant sur le bouton **Suivant**.

Paramètres du coffre-fort

Dans cette boîte de dialogue, vous pouvez définir les actions et les paramètres de coffre suivants :

- **Désignation du coffre-fort** : nom sous lequel le coffre est géré par le logiciel G DATA.
- **Description** : brève description supplémentaire des informations incluses dans le coffre, par exemple
- **Système de fichiers** : vous pouvez indiquer ici si le lecteur virtuel qui crée le coffre utilise le système de fichiers FAT ou NTFS. Il est généralement nécessaire de conserver ici l'option **Sélection automatique**.
- **Sélectionner automatiquement le lecteur du coffre-fort** : le coffre apparaît en tant que disque dur sur votre ordinateur. Vous pouvez saisir ici une lettre de lecteur pour le coffre et laisser le système lui attribuer automatiquement une lettre Nous vous recommandons de conserver ici l'option de sélection automatique.
- **Affecter le lecteur** : cette option est uniquement accessible si le logiciel ne choisit pas automatiquement le lecteur du coffre.

Cliquez maintenant sur le bouton **Suivant**.

Accès au coffre-fort

Vous pouvez définir ici un mot de passe pour le coffre. Pour ce faire, cliquez sur le bouton **Ajouter**.

Dans la boîte de dialogue qui s'affiche, saisissez le mot de passe souhaité sous **Mot de passe** et **Confirmer le mot de passe**. Le mot de passe n'est accepté que lorsque les deux champs saisis sont identiques. Cela vous permet de ne pas enregistrer de mot de passe erroné (faute de frappe, par exemple), que vous ne pourriez pas saisir de nouveau par la suite.

Cliquez sur **Ajouter** pour activer le mot de passe, puis sur **Suivant** pour terminer la configuration du coffre.

> **Remarque** : lors de la création d'un coffre, vous pouvez également définir différents mots de passe pour différentes autorisations. Vous pouvez, par exemple, créer un coffre dont vous pouvez lire et modifier les fichiers et fournir un autre mot de passe aux autres personnes, afin qu'elles puissent également lire le contenu du coffre, mais pas le modifier.

Si, une fois le coffre créé, vous le sélectionnez et cliquez sur le bouton **Autorisations**, les possibilités de paramétrage suivantes s'offrent à vous :

- **Exécuter le démarrage automatique** : chaque coffre contient un répertoire avec pour nom Programme de démarrage automatique. Si cette option reste réglée sur Oui, tous les fichiers exécutables inclus sont automatiquement lancés à l'ouverture du coffre.
- **Ouverture en lecture seule** : un utilisateur se connectant avec la méthode d'accès Lecture seule ne pourra ni enregistrer, ni modifier les fichiers du coffre-fort. Il ne peut que les lire.
- **Ouvrir en tant que support amovible** : le logiciel G DATA ouvre les coffres de données dans l'Explorateur comme s'il s'agissait de disques durs locaux. Si vous souhaitez que le coffre-fort soit visible dans le système en tant que support amovible, veuillez sélectionner cette option.
- **Utilisation commune** : la sélection de cette option permet l'utilisation commune du répertoire du coffre-fort par les autres ordinateurs du réseau. Avertissement : avec cette option, il est possible d'accéder au coffre sans saisir de mot de passe. Nous recommandons de réfléchir prudemment et en conscience de cause avant de choisir l'utilisation partagée du coffre-fort. L'utilisation partagée du coffre-fort pour tous les participants du réseau est dans ce cas judicieuse car les données sont accessibles à tout un chacun.
- **Fermer le coffre-fort après déconnexion de l'utilisateur** : cette option doit généralement être activée car si le coffre-fort reste ouvert après la déconnexion de l'utilisateur, d'autres utilisateurs peuvent en consulter le contenu.
- **Coffre-fort automatique** : tous les coffres-forts disposant de cette propriété peuvent être ouverts à l'aide d'une commande.

Configuration du coffre-fort

L'assistant de création pour coffre-fort vous communique les paramètres de réglage lors de la dernière étape. Si vous souhaitez modifier ces paramètres, cliquez sur le bouton **Précédent**. Si vous n'êtes pas satisfait de ces paramètres, cliquez sur **Créer**.

Le coffre de données virtuel et chiffré est créé sur le disque dur de votre ordinateur. Cliquez sur le bouton **Terminer le processus** pour créer le coffre et l'ouvrir directement (si vous le souhaitez).

Créer un coffre-fort mobile

Dès qu'un coffre est créé, vous pouvez le convertir en coffre portable. Vous pouvez le configurer de manière à pouvoir l'utiliser sur une clé USB ou à l'envoyer par courrier électronique.

Dans la vue d'ensemble des coffres de données, sélectionnez un coffre et cliquez ensuite sur le bouton **Créer un coffre-fort mobile**. Une boîte de dialogue qui vous aide à créer le coffre portable s'affiche alors. Cliquez sur **Suivant** pour procéder à la création.

Paramètres du coffre-fort

Vous avez ici la possibilité de modifier le mode d'attribution des paramètres pour les coffres standard. Les possibilités de paramétrage sont toutefois limitées pour les coffres portables :

- **Sélectionner automatiquement le lecteur du coffre-fort** : lorsque le coffre est ouvert, il apparaît en tant que disque dur. Vous pouvez saisir ici une lettre de lecteur pour le coffre et laisser le système lui attribuer automatiquement une lettre Nous vous recommandons de conserver ici l'option de sélection automatique.

- **Relier le coffre-fort au support de données** : vous pouvez indiquer ici que vous souhaitez uniquement utiliser le coffre portable avec la clé USB ou le disque dur sur laquelle ou lequel il a été créé, par exemple. Si le coffre n'est pas associé au support de données, vous pouvez également envoyer le fichier du coffre (qui présente l'extension **tsnxg**) en tant que pièce jointe à un courrier électronique ou le déplacer/copier sur un autre support de données, par exemple.

Support

Indiquez ici le support sur lequel le coffre portable doit être enregistré. Il peut s'agir d'une clé USB, d'un disque dur externe ou d'un CD/DVD.

> **Remarque** : si vous enregistrez le coffre sur un CD ou un DVD, vous ne pouvez bien évidemment qu'ouvrir et lire le coffre. Il n'est pas possible de modifier les fichiers et les répertoires du coffre sur ce type de supports de données.

Taille du coffre-fort

Cette rubrique vous indique la quantité d'espace mémoire dont le coffre a besoin sur le support de données cible. Si l'espace mémoire requis est trop important, vous pouvez annuler la création du coffre portable.

> **Remarque** : s'ajoutent à la taille du coffre environ 6 Mo de données de pilote, qui permettent l'ouverture du coffre sur les systèmes Windows sur lesquels le logiciel G DATA n'est pas installé.

Terminer

Pour finaliser la création du coffre portable, cliquez sur le bouton **Terminer le processus**. Si vous le souhaitez, vous pouvez maintenant afficher dans le navigateur le fichier dans lequel se trouve le coffre portable sur le support mémoire souhaité.

Ouvrir un coffre portable

Si vous souhaitez ouvrir un coffre portable sur un ordinateur Windows sur lequel le module de coffres de données G Data n'est pas installé, vous pouvez accéder aux données en sélectionnant, sur la clé USB, le disque dur mobile ou le CD/DVD, le fichier **start.exe** ou **start** dans le dossier **TSNxG_4**. Une boîte de dialogue qui vous permet d'ouvrir ou (si le coffre est déjà ouvert) de fermer le coffre s'affiche alors.

> **Attention** : si le coffre de données G DATA est utilisé pour la première fois sur un ordinateur, les données du pilote et les éléments de programme adaptés sont chargés. Un redémarrage est ensuite indispensable. Une fois l'ordinateur redémarré, sélectionnez de nouveau l'entrée **start** ou **start.exe**.

Saisissez votre mot de passe ou utilisez une des autres méthodes d'accès.

Le coffre-fort s'ouvre désormais et le contenu peut être utilisé.

Après le succès de votre connexion au coffre-fort, l'icone du coffre-fort s'affiche dans l'explorateur Windows à côté du lecteur local en tant que lecteur supplémentaire doté d'une lettre de lecteur correspondante. Chaque utilisateur de coffre-fort mobile peut transférer des données du coffre-fort sur l'ordinateur. Dans le cas d'une utilisation de coffre-fort mobile sur un support de données USB ou Flash Memory, l'utilisateur doté des autorisations en rapport peut copier les données du coffre-fort de l'ordinateur sur le coffre-fort.

La procédure de fermeture du coffre mobile est similaire à celle d'ouverture. Double-cliquez sur la lettre du lecteur du coffre ou

sélectionnez la commande correspondante d’un clic droit de la souris dans le menu contextuel.

> **Attention** : Il est recommandé de fermer le coffre-fort après le succès d'une action avant de retirer le support de données mobile. Accédez pour ce faire au support de données portable, ouvrez le répertoire G DATA et cliquez sur start.exe. Une boîte de dialogue vous permettant de fermer le coffre s’affiche alors.

Autostart Manager

L’application Autostart Manager permet de gérer les programmes lancés automatiquement au démarrage de Windows. Ces programmes sont normalement directement chargés au démarrage du système. S’ils sont gérés dans l’application Autostart Manager, ils peuvent être lancés de manière retardée ou en fonction de la charge du système ou du disque dur. Cela permet de démarrer plus rapidement le système et d’améliorer ainsi les performances de l’ordinateur.

Lorsque vous ouvrez l’application Autostart Manager, la liste de tous les programmes installés sur votre ordinateur qui disposent de la fonction de démarrage automatique s’affiche sur la gauche. Ces programmes démarrent normalement immédiatement, lorsque le système Windows est lancé, et peuvent donc ralentir le démarrage de votre ordinateur.



Il vous suffit de sélectionner avec l’icône en forme de flèche les programmes disposant de la fonction de démarrage automatique que vous souhaitez lancer de manière retardée pour rééquilibrer le processus de démarrage du système Windows. Votre système d’exploitation Windows est ainsi lancé et prêt bien plus rapidement.



Si vous souhaitez de nouveau lancer immédiatement un programme disposant de la fonction de démarrage automatique, il vous suffit de le transférer du dossier **Lancement automatique retardé** au dossier **Lancement automatique immédiat**.

Définir le retard

Une fois un programme placé dans le dossier Lancement automatique retardé, vous pouvez définir à l’issue de combien de minutes le logiciel doit être lancé. Il vous suffit de cliquer sur le programme et de sélectionner le laps de temps souhaité dans la colonne Retard.

Les entrées suivantes sont ici à votre disposition :

- **Ne pas lancer** : l’application est gérée par l’application Autostart Manager, elle n’est pas lancée au redémarrage du système. Elle reste inactive.
- **1 - 10 minutes** : l’application démarre à l’issue du laps de temps indiqué ici.
- **Démarrage automatique** : l’application démarre automatiquement, en fonction de la charge de l’unité centrale/du disque dur. Cela signifie que les applications disposant de la fonction de démarrage automatique ne sont lancées que lorsque le système n’est plus surchargé par le lancement d’autres applications ou d’autres processus.

Propriétés

Si vous double-cliquez sur l’entrée d’un programme figurant dans la liste de l’application Autostart Manager, des informations complètes au sujet du logiciel géré s’affichent.

Contrôle des périphériques

Le contrôle des périphériques vous permet de définir les supports mémoire autorisés en lecture et/ou en écriture sur votre ordinateur. Vous pouvez également empêcher le transfert de données privées sur une clé USB ou leur gravure sur un CD. De plus, vous pouvez indiquer précisément les supports de données amovibles (clés USB ou disques durs USB externes, par exemple) sur lesquels les données peuvent être téléchargées. Vous pouvez ainsi utiliser votre disque dur USB pour la sauvegarde de données sans que les autres disques durs aient accès à ces données.

Cette vue d’ensemble vous permet de déterminer les effets des paramètres du contrôle des périphériques pour l’utilisateur concerné. Le bouton Modifier les règles vous permet de modifier à votre guise les paramètres pour le périphérique et l’utilisateur.

Paramètres

La rubrique **Paramètres** vous permet de configurer le module du programme à votre guise. Il n'est généralement pas nécessaire d'apporter des modifications, le logiciel G DATA étant déjà configuré de manière optimale pour le système lors de l'installation. Les fonctions générales suivantes sont disponibles pour les paramètres :



Enregistrer les paramètres : vous pouvez enregistrer les paramètres définis dans un fichier de paramètres G DATA. Si vous utilisez le logiciel G DATA sur plusieurs ordinateurs, vous pouvez ainsi définir des paramètres sur un ordinateur, les enregistrer et charger le fichier de paramètres sur les autres ordinateurs.



Charger les paramètres : vous pouvez charger le fichier de paramètres G DATA créé sur cet ordinateur ou sur un autre.



Réinitialiser les paramètres : ce bouton vous permet de réinitialiser tous les paramètres du logiciel G DATA en cas d'erreur. Vous pouvez décider de réinitialiser toutes les rubriques de paramètres ou uniquement certaines. Il vous suffit d'activer la case à cocher des rubriques que vous souhaitez réinitialiser.

Généralités

Sécurité / Performance

Si vous souhaitez utiliser votre protection antivirus sur un ordinateur lent, vous avez la possibilité d'améliorer le niveau de sécurité au profit des performances, ainsi que de la vitesse de fonctionnement de l'ordinateur. Le schéma vous montre les effets d'une optimisation des paramètres.

- **Ordinateur standard (recommandé)** : vous bénéficiez ici de la protection optimale du logiciel G DATA. Les deux moteurs antivirus du programme fonctionnent conjointement. Tous les accès en lecture et en écriture de l'ordinateur sont vérifiés afin de s'assurer de l'absence de code nuisible.

  Moteur : le logiciel G DATA fonctionne avec deux moteurs antivirus. En principe, l'utilisation de ces deux moteurs garantit une prophylaxie optimale.

- **Ordinateur lent** : le logiciel G DATA peut également ne fonctionner qu'avec un seul moteur de manière à ne pas nuire à la vitesse de fonctionnement sur les ordinateurs lents. De nombreux programmes antivirus disponibles sur le marché ne vous proposent que cette protection parce qu'ils ne fonctionnent qu'avec un seul moteur. La protection est donc toujours correcte. Vous pouvez également indiquer que lorsque le mode de protection antivirus est activé, l'analyse ne doit être effectuée qu'en cas de processus d'écriture. Seules les données qui viennent d'être enregistrées sont ainsi vérifiées, ce qui optimise encore davantage les performances.

- **Défini par l'utilisateur** : vous pouvez indiquer ici si vous souhaitez utiliser un moteur ou les deux et si la protection antivirus doit être utilisée pour les processus d'écriture et de lecture, uniquement pour les processus d'écriture (Exécuter), voire pas du tout (déconseillé).

Mot de passe

Vous pouvez, via l'attribution d'un mot de passe, protéger les paramètres de votre logiciel G DATA. Aucun autre utilisateur de votre ordinateur ne peut ainsi désactiver la protection antivirus ou l'analyse en cas d'inactivité, par exemple.

Pour définir un mot de passe, vous devez le saisir sous Mot de passe, puis sous Confirmer le mot de passe, de manière à exclure toute faute de frappe. Vous pouvez également saisir une remarque concernant le mot de passe sous Remarque sur le mot de passe.

Remarque : la remarque relative au mot de passe s'affiche en cas de saisie incorrecte. Elle fournit des indications permettant de se rappeler du mot de passe.

Remarque : la protection par mot de passe offre une protection complète du logiciel. Pour bénéficier d'une sécurité maximale, vous devez travailler avec plusieurs comptes utilisateur. Vous pouvez ainsi, en tant qu'administrateur, gérer la protection antivirus au niveau de votre compte utilisateur, par exemple. Les autres utilisateurs (enfants, amis ou parents, par exemple) disposent de comptes utilisateur avec des droits limités et ne peuvent donc apporter aucune modification à la protection antivirus.

Remarque : si, une fois les différents comptes utilisateur créés, par exemple, vous n'avez plus besoin de mot de passe pour votre logiciel G DATA, vous pouvez supprimer l'obligation de saisie d'un mot de passe à l'aide du bouton Supprimer le mot de passe.

AntiVirus

Protection temps réel

La protection antivirus en temps réel analyse l'ensemble de votre ordinateur à la recherche de virus ; elle contrôle les procédures d'écriture et de lecture et dès qu'un programme souhaite exécuter des fonctions nuisibles ou diffuser des fichiers malveillants, il est bloqué par la protection antivirus. Le gardien est votre principale protection ! La protection antivirus ne doit jamais être désactivée !

Les options suivantes sont ici à votre disposition :

- **Statut de l'outil de surveillance** : indiquez ici si le gardien doit être activé ou désactivé.
- **Utiliser les moteurs** : le logiciel fonctionne avec deux moteurs, deux programmes de vérification antivirus fonctionnant indépendamment l'un de l'autre. Chaque moteur en lui-même vous garantit déjà une très grande protection contre les virus mais la combinaison des deux moteurs livre des résultats encore plus exceptionnels. Sur les ordinateurs anciens et lents, l'utilisation d'un seul moteur permet d'accélérer la vérification antivirus mais en règle générale, il vous est recommandé de conserver le paramètre **Les deux moteurs**.
- **Fichiers infectés** : dans le cadre du paramétrage par défaut, lorsqu'un virus est détecté, le logiciel vous demande ce que vous souhaitez faire du virus et du fichier infecté. Si vous souhaitez toujours réaliser la même action, vous pouvez procéder ici au réglage correspondant. Le paramètre **Désinfecter (sinon : envoyer en quarantaine)** offre, à ce titre, une sécurité optimale pour vos données.
- **Archives infectées** : indiquez ici si les fichiers d'archive (les fichiers avec l'extension RAR, ZIP ou encore PST, par exemple) ne doivent pas être traités comme les fichiers normaux. Nous attirons cependant votre attention sur le fait que l'ajout d'une archive à la quarantaine peut endommager celle-ci au point qu'elle ne puisse plus être utilisée, même une fois placée hors de la **Quarantaine**.
- **Surveillance du comportement** : si la surveillance comportementale est activée, chaque activité du système est surveillée, indépendamment du gardien. Ce qui permet de détecter les programmes nuisibles pour lesquels il n'existe pas encore de signature.
- **Exploit Protection** : les exploits utilisent les failles des logiciels les plus courants et peuvent ainsi prendre le contrôle de votre ordinateur dans le pire des cas. Les exploits peuvent attaquer le système, même lorsque les applications (outil d'affichage des fichiers PDF, navigateur, etc.) sont régulièrement mises à jour. La fonction Exploit Protection vous protège contre de tels accès, elle assure également une protection proactive contre les attaques encore inconnues.

Exceptions

Vous pouvez exclure certains lecteurs, répertoires et fichiers de la vérification et accélérer ainsi considérablement la détection des virus en cliquant sur le bouton Exceptions.

Pour cela, procédez comme suit :

1. Cliquez sur le bouton **Exceptions**.
2. Dans la fenêtre **Exceptions du gardien**, cliquez sur **Nouveau**.
3. Indiquez à présent si vous souhaitez exclure un lecteur, un répertoire, un fichier ou un type de fichiers.
4. Sélectionnez le répertoire ou le lecteur que vous souhaitez protéger. Pour protéger les fichiers, saisissez le nom complet du fichier dans la zone de saisie du formulaire. Vous pouvez également travailler ici avec des caractères génériques.

   Remarque : Les caractères de remplacement fonctionnent comme suit :

   - L'icône en forme de point d'interrogation (?) représente des caractères uniques.
   - L'astérisque (*) remplace des suites de caractères.

   Par exemple, pour protéger tous les dossiers .sav, saisissez *.sav. Afin de protéger une sélection spéciale de fichiers comprenant des noms de fichiers successifs (par exemple, text1.doc, text2.doc, text3.doc), saisissez text?.doc.

Vous pouvez répéter aussi souvent que vous le souhaitez cette procédure et supprimer ou modifier les exceptions existantes.

Avancé

Définissez, en outre, en cliquant sur **Avancé**, les analyses supplémentaires devant être réalisées par le gardien.

En règle générale, vous n'avez pas à procéder à d'autres paramétrages.

- **Mode** : vous pouvez indiquer ici si les fichiers doivent être vérifiés lors de l'exécution, lors de la lecture uniquement ou lors de l'écriture et de la lecture. Si la vérification a lieu lors de l'écriture du fichier, le logiciel vérifie, lors de la création d'un fichier ou d'une version de fichier, que le fichier n'a pas été infecté par un processus inconnu. Sinon, les fichiers sont uniquement vérifiés lors de la lecture par des programmes.

- **Surveillance particulière des dossiers critiques** : cette fonction permet de surveiller particulièrement les dossiers critiques, comme les dossiers partagés en réseau, les données personnelles ou les services dans le nuage (Microsoft Dropbox OneDrive, Google Drive, etc.). Une fois les dossiers critiques sélectionnés dans le champ de la boîte de dialogue, ils sont toujours surveillés en mode **Analyser lors de la lecture et de l'écriture**, indépendamment des paramètres utilisés pour les autres fichiers, dossiers et répertoires. Si vous avez sélectionné le mode **Analyser lors de la lecture et de l'écriture** pour tous les fichiers, le paramètre est grisé pour les dossiers critiques.

- **Vérifier les accès au réseau** : S'il existe, sur votre ordinateur, une connexion réseau vers des ordinateurs non protégés (par ex. ordinateurs portables externes), il est recommandé de vérifier également les accès au réseau afin de détecter un transfert éventuel de programmes malintentionnés. Si vous utilisez votre ordinateur comme ordinateur une place sans accès au réseau, cette option ne doit pas nécessairement être activée. Si vous avez installé sur tous les ordinateurs du réseau un programme antivirus, il est également recommandé de désactiver cette option car sinon, certains fichiers seront analysés deux fois, ce qui aura un effet négatif sur la vitesse.

- **Heuristique** : L'analyse heuristique permet non seulement de détecter les virus à l'aide des mises à jour antivirus, que nous mettons en ligne pour vous régulièrement, mais aussi les caractéristiques typiquement virales. Bien que ce paramètre ajoute à votre sécurité, il peut dans de rares cas déclencher une fausse alerte.

- **Vérifier les archives** : la vérification de données compressées dans des archives (on les reconnaît aux extensions de fichiers ZIP, RAR ou encore PST) nécessite beaucoup de temps et s'avère généralement inutile lorsque la protection antivirus est activée au niveau du système. Si vous souhaitez accélérer la vérification antivirus, vous pouvez limiter la taille des fichiers d'archive analysés à une certaine valeur en kilo-octets.

- **Analyser les archives de courriers électroniques** : le logiciel vérifiant déjà les courriers électroniques entrants et sortants, il est dans la plupart des cas plus logique d'omettre la vérification régulière des archives des messages électroniques. De plus, ce procédé peut prendre quelques minutes selon la taille des archives.

- **Analyser les zones du système au démarrage du système** : les différents volets comme les secteurs de démarrage ne doivent pas, normalement, être exclus du contrôle antivirus. Vous pouvez définir ici si elles sont vérifiées lors du démarrage du système ou lors d'un changement de mode de transmission de données (par ex. lors de l'insertion d'un nouveau CD-ROM). En règle générale, vous devriez activer au moins l'une de ces deux fonctions.

- **Analyser les zones du système lors du changement de support** : les différents volets comme les secteurs de démarrage ne doivent pas, normalement, être exclus du contrôle antivirus. Vous pouvez définir ici si elles sont vérifiées lors du démarrage du système ou lors d'un changement de support de données (lors de l'insertion d'un nouveau CD-ROM, par ex.). En règle générale, vous devriez activer au moins l'une de ces deux fonctions.

- **S'assurer de l'absence de composeurs/logiciels espions/logiciels publicitaires** : le logiciel permet également de détecter les composeurs et autres programmes nuisibles. Il peut s'agir de programmes établissant des connexions Internet onéreuses contre votre gré, programmes qui n'ont rien à envier au potentiel financièrement dévastateur des virus : ils peuvent, par exemple, enregistrer discrètement vos habitudes de navigation, voire l'ensemble de vos saisies clavier (y compris vos mots de passe), puis, la première occasion venue, utiliser Internet pour les transmettre à un tiers.

- **Analyser uniquement les nouveaux fichiers ou les fichiers modifiés** : lorsque cette fonction est activée, les fichiers qui n'ont pas été modifiés depuis longtemps et qui sont considérés comme inoffensifs ne sont pas vérifiés. Cela permet un gain de performances lors des tâches quotidiennes, sans risque pour la sécurité.

Analyse antivirus manuelle

Vous pouvez définir ici les paramètres de base du programme pour l' Analyse antivirus.

Ce n'est par contre pas nécessaire en fonctionnement normal.

- **Utiliser les moteurs** : le logiciel fonctionne avec deux moteurs, deux programmes de vérification antivirus synchronisés. Sur les ordinateurs anciens et lents, l'utilisation d'un seul moteur permet d'accélérer la vérification antivirus mais en règle générale, il vous est recommandé de conserver le paramètre **Les deux moteurs**.

- **Fichiers infectés** : votre logiciel a détecté un virus ? Dans le cadre du paramètre par défaut, le logiciel vous demande ce que vous voulez faire avec le virus et le fichier infecté. Si vous souhaitez toujours réaliser la même action, vous pouvez procéder ici au réglage correspondant. Le paramètre **Désinfecter (sinon : envoyer en quarantaine)** offre, à ce titre, une sécurité optimale pour vos données.

- **Archives infectées** : indiquez ici si les fichiers d'archive (les fichiers avec l'extension RAR, ZIP ou encore PST, par exemple) ne doivent pas être traités comme les fichiers normaux. Nous attirons cependant votre attention sur le fait que l'ajout d'une archive à la quarantaine peut endommager celle-ci au point qu'elle ne puisse plus être utilisée, même une fois placée hors de la **Quarantaine**.

- **En cas de surcharge du système, mettre l'analyse antivirus en pause** : Normalement, une analyse antivirus devrait être effectuée lorsque vous n'utilisez pas l'ordinateur. Si néanmoins vous utilisiez l'ordinateur, l'analyse antivirus se met en pause afin de pouvoir utiliser votre ordinateur à sa puissance habituelle. L'analyse antivirus s'effectue donc à des moments où vous ne travaillez pas.

Exceptions

Vous pouvez exclure certains lecteurs, répertoires et fichiers de la vérification et accélérer ainsi considérablement la détection des virus en cliquant sur le bouton Exceptions.

Pour cela, procédez comme suit :

1. Cliquez sur le bouton **Exceptions**.

2. Dans la fenêtre **Exceptions à la vérification manuelle de l'ordinateur**, cliquez sur **Nouveau**.

3. Indiquez à présent si vous souhaitez exclure un lecteur, un répertoire, un fichier ou un type de fichiers.

4. Sélectionnez le répertoire ou le lecteur que vous souhaitez protéger. Pour protéger les fichiers, saisissez le nom complet du fichier dans la zone de saisie du formulaire. Vous pouvez également travailler ici avec des caractères génériques.

   Remarque : Les caractères de remplacement fonctionnent comme suit :

   - L'icône en forme de point d'interrogation (?) représente des caractères uniques.

   - L'astérisque (*) remplace des suites de caractères.

   Par exemple, pour protéger tous les dossiers .sav, saisissez *.sav. Afin de protéger une sélection spéciale de fichiers comprenant des noms de fichiers successifs (par exemple, text1.doc, text2.doc, text3.doc), saisissez text?.doc.

Vous pouvez répéter aussi souvent que vous le souhaitez cette procédure et supprimer ou modifier les exceptions existantes.

Utiliser également pour le ScanDiscret : alors que, lors de la vérification antivirus manuelle, l'ordinateur est analysé de manière ciblée et ne peut être utilisé pour d'autres tâches, l'analyse en cas d'inactivité est une vérification antivirus intelligente qui vérifie que les fichiers de votre ordinateur ne sont pas déjà infectés par un virus. Le scan discret fonctionne de manière similaire à un économiseur d'écran, lorsque vous n'utilisez pas votre ordinateur depuis un moment. Il s'arrête dès que vous reprenez le travail afin de vous garantir des performances optimales. Vous pouvez définir ici si des fichiers ou des répertoires d'exceptions doivent également être définis pour le scan discret.

Avancé

En cliquant sur le bouton Avancé, vous pouvez définir des paramètres avancés d'analyse antivirus.

Dans la plupart des cas cependant, l'utilisation des paramètres standard définis suffit largement.

- **Types de fichiers** : vous pouvez définir ici quels types de fichiers seront analysés par le logiciel G DATA. La sélection de l'option Fichiers programmes et documents uniquement apporte un avantage en termes de vitesse d'exécution.
- **Heuristique** : lorsque l'analyse heuristique est utilisée, les virus sont reconnus non seulement par le biais de la base de données des virus que vous obtenez avec chaque mise à jour du logiciel antivirus, mais également au moyen de certaines caractéristiques typiques aux virus. Bien que ce paramètre ajoute à votre sécurité, il peut dans de rares cas déclencher une fausse alerte.
- **Vérifier les archives** : la vérification de données compressées dans des archives (on les reconnaît aux extensions de fichiers ZIP, RAR ou encore PST) nécessite beaucoup de temps et s'avère généralement inutile lorsque la protection antivirus est activée au niveau du système. Si vous souhaitez accélérer la vérification antivirus, vous pouvez limiter la taille des fichiers d'archive analysés à une certaine valeur en kilo-octets.
- **Analyser les archives de courriers électroniques** : cette option vous permet de déterminer si les archives de messagerie doivent également être analysées.
- **Analyser les rubriques du système** : les différents volets comme les secteurs de démarrage ne doivent pas, normalement, être exclus du contrôle antivirus.
- **S'assurer de l'absence de composeurs/logiciels espions/logiciels publicitaires** : cette fonction permet de détecter les composeurs et autres logiciels malveillants. Il peut s'agir de programmes établissant des connexions Internet onéreuses contre votre gré, programmes qui n'ont rien à envier au potentiel financièrement dévastateur des virus : ils peuvent par exemple enregistrer discrètement vos habitudes de navigation, voire l'ensemble de vos saisies clavier (y compris vos mots de passe), puis, la première occasion venue, utiliser Internet pour les transmettre à un tiers.
- **Détecter les RootKits** : les trousses administrateur pirate tentent d'esquiver les méthodes de détection habituelles des virus. Un contrôle supplémentaire à la recherche de ces logiciels malveillants est toujours recommandé.
- **Analyser uniquement les nouveaux fichiers ou les fichiers modifiés** : lorsque cette fonction est activée, les fichiers qui n'ont pas été modifiés depuis longtemps et qui sont considérés comme inoffensifs ne sont pas vérifiés. Cela permet un gain de performances lors des tâches quotidiennes, sans risque pour la sécurité.
- **Inscrire dans le journal** : cette case à cocher vous permet d'indiquer que le logiciel doit créer un protocole lors de la vérification antivirus. Il est possible de le consulter ensuite dans la rubrique Protocoles.
- **Proposer l'analyse des virus pour les supports de données amovibles** : si cette case à cocher est activée, lors de la connexion d'un support de données amovible (clé USB, disque dur externe, etc.) à votre ordinateur, le système vous demande si une analyse antivirus du périphérique doit être effectuée.

Mises à jour

Si la mise à jour Internet du logiciel ou des signatures antivirus ne fonctionne pas, vous pouvez saisir dans cette rubrique toutes les données indispensables à une mise à jour automatique. Saisissez dans les options les données d'accès (nom d'utilisateur et mot de passe) que vous avez reçues par courrier électronique lors de l'enregistrement en ligne de votre logiciel. Grâce à ces données, le serveur de mise à jour G Data vous identifie et les actualisations peuvent désormais s'effectuer de manière entièrement automatique.

Si vous disposez d'une nouvelle licence que vous souhaitez activer, sélectionnez **Activer la licence**. Les **Paramètres Internet** affichent des options spécifiques dont vous n'avez besoin que dans des cas exceptionnels (serveur proxy, autre région). Vous ne devez désactiver la vérification de la version que de manière temporaire, lorsque vous rencontrez des problèmes dans le cadre de la mise à jour des signatures antivirus.

> **Importation/exportation des signatures antivirus** : sur les ordinateurs rarement ou jamais connectés à Internet ou s'il existe des limites en matière de volumes de données pour les téléchargements, vous pouvez actualiser les signatures antivirus via un support de données (clé USB, par exemple). En d'autres termes, vous pouvez procéder à une **mise à jour hors ligne**. Pour ce faire, vous devez exporter les signatures antivirus d'un ordinateur connecté à Internet et disposant des droits nécessaires vers le support de données. Vous pouvez ensuite importer les signatures sur un ordinateur sans connexion Internet, à l'aide de la fonction Importer de. Le système de cet ordinateur est alors protégé à l'aide des dernières signatures antivirus. Contrairement aux mises à jour des signatures antivirus régulièrement effectuées par Internet, l'utilisateur est ici impliqué et doit veiller à procéder à des signatures antivirus aussi souvent que possible.

Actualisation automatique des signatures de virus

Désactivez la case à cocher si vous ne souhaitez pas que le logiciel G Data se charge automatiquement de la mise à jour des signatures antivirus. La désactivation de cette fonction représente toutefois un risque plus élevé pour la sécurité et ne doit avoir lieu que de manière exceptionnelle. Si vous estimez que l'intervalle entre les mises à jour est trop réduit, vous pouvez modifier ce paramètre et déterminer que la mise à jour a uniquement lieu lors de la connexion Internet, par exemple. Cette option est utile pour les ordinateurs qui ne sont pas connectés en permanence à Internet, par exemple.

Inscrire dans le journal : si vous activez cette case à cocher, chaque mise à jour des signatures antivirus est incluse dans le protocole, que vous pouvez afficher au niveau des fonctions complémentaires du logiciel G DATA (dans le **SecurityCenter** sous **Protocoles**). Le protocole inclut, en plus de ces entrées, des informations relatives aux virus détectés et autres actions effectuées par le programme.

Activer la licence

Si vous n'avez pas encore enregistré votre logiciel G DATA, vous pouvez procéder maintenant à son enregistrement en saisissant votre numéro d'enregistrement et vos données client. Selon le type de produit, le numéro d'enregistrement est indiqué au verso du manuel d'utilisation, dans le courrier de confirmation du téléchargement du logiciel ou sur la pochette du CD. La saisie du numéro d'enregistrement permet d'activer le produit.

Cliquez maintenant sur le bouton **Se connecter**, vos données d'accès sont générées sur le serveur de mise à jour. En cas de succès de la connexion, le programme affiche le message **La connexion a été établie avec succès**, que vous pouvez fermer en cliquant sur le bouton Fermer.

> **Attention** : vos données d'accès vous sont également envoyées par courrier électronique à des fins d'information et pour une éventuelle réinstallation du logiciel. Pour cette raison, veuillez vous assurer que l'adresse e-mail communiquée lors de l'enregistrement en ligne est correcte. Dans le cas contraire, vous ne pourriez pas disposer de vos données d'accès.

Les données d'accès sont automatiquement reprises dans le formulaire de saisie initial et vous pouvez désormais mettre les signatures antivirus à jour via Internet.

> **Vous ne parvenez pas à activer votre licence ?** Si vous ne parvenez pas à vous connecter au serveur, il est possible que le problème se trouve au niveau du serveur proxy. Cliquez sur le bouton **Paramètres Internet**. Vous pouvez définir ici les paramètres de votre connexion Internet. En cas de problèmes lors de la mise à jour des signatures antivirus, vous devez commencer par vérifier que vous pouvez vous connecter à Internet à l'aide d'un navigateur (Internet Explorer, par exemple). Si vous ne parvenez pas à vous connecter à Internet, le problème est sans doute lié à la connexion Internet et non aux données du serveur proxy.

Paramètres Internet

Si vous utilisez un serveur proxy, activez la case à cocher **Utiliser le serveur proxy**. Vous ne devez modifier ce réglage que si la mise à jour des signatures antivirus ne fonctionne pas. Pour toute question concernant l'adresse proxy, veuillez vous adresser à votre administrateur système ou votre fournisseur d'accès à Internet. Si nécessaire, vous pouvez également saisir ici les données d'accès pour le serveur proxy.

> **Serveur Proxy** : le serveur proxy recueille les demandes réseau et les transmet à l'ordinateur connecté. Ainsi, si vous utilisez par exemple votre ordinateur dans un réseau d'entreprise, il peut être utile de se connecter au réseau via un serveur proxy. En cas de problèmes lors de la mise à jour des signatures antivirus, vous devez commencer par vérifier que vous pouvez vous connecter au réseau à l'aide d'un navigateur Internet. Si vous ne parvenez pas à vous connecter à Internet, le problème est sans doute lié à la connexion Internet et non aux données du serveur proxy.

Protection Internet

Lorsque la protection Web est activée, elle vérifie que les contenus Internet ne présentent pas de logiciels malveillants pendant la navigation. Vous pouvez définir ici les paramètres suivants.

- **Vérifier les contenus Internet (HTTP)** : les options de la protection Web vous permettent de vérifier que les contenus Web HTTP ne sont pas infectés pendant la navigation. Les contenus Internet infectés ne seront pas parcourus et les pages correspondantes ne seront pas affichées. Pour ce faire, vous devez activer la case à cocher **Vérifier les contenus Internet (HTTP)**.

  Si vous ne souhaitez pas procéder à la vérification des contenus Internet, la protection antivirus intervient tout de même lors du lancement de fichiers infectés. Votre système demeure donc aussi protégé sans analyse des contenus Internet, tant que l'outil de surveillance antivirus est activé.

  Vous pouvez également définir certains sites Web en tant qu'exceptions, si vous les considérez comme inoffensifs. Pour de plus amples informations à ce sujet, reportez-vous au chapitre **Déterminer exceptions**. Le bouton **Avancé** vous permet de définir d'autres paramètres concernant le traitement des contenus Internet.

- **Protection anti-hameçonnage** : les tentatives d'hameçonnage ont pour but d'attirer les clients d'une banque ou d'un magasin vers un faux site Internet sur lequel leurs données personnelles sont volées. Il est fortement recommandé d'activer ce dispositif de protection anti-hameçonnage.

- **Envoyer les adresses des sites Internet infectés** : cette fonction vous permet, sous le couvert de l'anonymat bien évidemment, de signaler automatiquement les pages Internet considérées par le logiciel comme dangereuses. Ainsi vous optimisez la sécurité de tous les utilisateurs.

- **Protection du navigateur BankGuard** : Les chevaux de Troie bancaires constituent une menace toujours plus grande. Les cybercriminels développent, en quelques heures, de nouvelles variantes de codes malveillants (ZeuS, SpyEye) dans le but de dérober votre argent. Les banques sécurisent leur trafic de données sur Internet, les données sont cependant déchiffrées au niveau du navigateur Internet du client, là où interviennent les chevaux de Troie bancaires. La technologie de l'application G Data BankGuard protège cependant vos opérations bancaires dès qu'elles sont initiées et précisément là où les attaques ont lieu. La vérification de l'authenticité des bibliothèques réseau utilisées permet à la technologie G Data BankGuard de s'assurer que votre navigateur Internet n'est pas manipulé par un cheval de Troie bancaire. Nous vous recommandons d'activer en permanence la protection G Data BankGuard.

- **Protection contre les enregistreurs de frappe** : la protection contre les enregistreurs de frappe détermine, indépendamment des signatures antivirus, si la saisie au clavier est espionnée sur votre système. Les pirates ont alors la possibilité d'enregistrer vos mots de passe. Cette fonction doit toujours rester activée.

Déterminer exceptions

Procédez comme suit pour ajouter une page Internet comme exception dans la liste blanche :

1. Cliquez sur le bouton **Déterminer exceptions**. La fenêtre de la liste blanche apparaît alors. Ici s'affichent les pages Internet que vous avez sélectionnées comme fiables et placées ici.

2. Pour ajouter une autre page Internet, cliquez sur le bouton **Nouveau**. Un masque de saisie s'ouvre. Saisissez l'adresse du site Web (www.site inoffensif.fr, par exemple) sous **Adresse URL** et la raison pour laquelle vous souhaitez ajouter ce site Web, le cas échéant, sous **Remarque**. Confirmez la saisie en cliquant sur **OK**.

3. Confirmez maintenant toutes les modifications apportées à la liste blanche en cliquant sur **OK**.

Pour supprimer une page Internet de la liste blanche, sélectionnez celle-ci dans la liste avec la souris et cliquez simplement sur le bouton **Supprimer**.

Avancé

Vous pouvez définir ici les numéros de port du serveur qui doivent être surveillés par la protection Web. Dans le cadre d'une surveillance de navigation normale, il suffit généralement de saisir ici le numéro de port 80.

- **Éviter les dépassements de temps dans le navigateur** : étant donné que le logiciel traite les contenus Internet avant leur affichage dans le navigateur Internet, ce qui peut nécessiter un certain temps selon le chargement de données, un message d'erreur peut apparaître dans le navigateur Internet s'il ne reçoit pas immédiatement les données envoyées, car elles doivent faire l'objet d'une analyse par le logiciel antivirus à la recherche de routines préjudiciables. Si vous activez la case à cocher **Ne pas dépasser la limite de temps dans le navigateur**, le message d'erreur est bloqué et les données du navigateur sont transmises tout à fait normalement après avoir été soumises à une analyse antivirus.

- **Limitation de la taille pour les téléchargements** : permet d'interrompre la vérification HTTP des contenus Web trop volumineux. Les contenus des pages seront analysés par l'outil de surveillance antivirus si des routines nuisibles s'activent. La limitation de taille présente l'avantage d'empêcher le ralentissement de votre navigation sur Internet à cause des contrôles antivirus.

Analyse de la messagerie électronique

La fonction d'analyse du courrier électronique vous permet de vérifier la présence de virus dans les courriers électroniques entrants et sortants ainsi que dans leurs pièces jointes et d'éliminer ainsi les infections éventuelles directement à la source. Si un virus est détecté dans une pièce jointe, le logiciel peut le supprimer ou réparer les fichiers infectés.

> **Attention** : dans Microsoft Outlook, l'analyse des courriers électroniques repose sur un plugiciel. Ce dernier offre la même sécurité que la fonction de protection des programmes de messagerie POP3/IMAP dans les options antivirus. Une fois ce plugiciel installé, le menu Outlook **Outils** inclut la fonction **Rechercher des virus dans un dossier**, qui vous permet de vérifier que les dossiers de messages ne sont pas infectés.

Courriers entrants

Les options suivantes vous permettent de procéder à l'analyse antivirus des courriers électroniques entrants :

- **En cas de contamination** : Vous pouvez ici définir ce qui doit se produire en cas de découverte d'un message infecté. Les différentes options de paramètres sont utiles en fonction de votre motif d'utilisation de l'ordinateur. En règle générale, il est recommandé de sélectionner le paramètre **Désinfecter (si cela n'est pas possible : supprimer le texte/la pièce jointe**.

- **Vérifier les courriers reçus** : si vous activez cette option, tous les messages électroniques que vous recevez lorsque vous travaillez sur l'ordinateur sont analysés.

- **Joindre un rapport concernant les courriers électroniques reçus contaminés** : Si vous avez activé l'option de rapports, **VIRUS** s'affiche dans la ligne d'objet du courriel infecté en cas de détection de virus et le message **Attention ! Ce message est infecté par les virus suivants**, suivi du nom du virus ainsi que la précision que le virus a été supprimé ou non ou que le fichier infecté a pu être réparé ou non, s'affiche au début du corps du message.

Courriers sortants

Pour que vous ne transmettiez pas accidentellement des virus, le logiciel vous offre également la possibilité de vous assurer de l'absence de virus dans vos courriers électroniques avant envoi. Si un courriel que vous voulez envoyer contient un virus, le programme affiche le message **Le courriel [ligne de l'objet] contient le virus suivant : [Nom du virus]**. Le courriel correspondant ne peut pas être envoyé et n'est pas envoyé. Pour vérifier les courriers électroniques sortants, activez la case à cocher **Analyser les courriers électroniques avant envoi**.

Options d'analyse

Vous pouvez activer ou désactiver ici les options de base de la vérification antivirus :

- **Utiliser les moteurs** : le logiciel fonctionne avec deux moteurs antivirus, deux unités d'analyse synchronisées. En principe, l'utilisation de ces deux moteurs garantit une prophylaxie optimale.

- **OutbreakShield** : cette case vous permet d'activer la protection AntiVirus OutbreakShield. Si la fonction OutbreakShield est activée, le logiciel établit des sommes de contrôle des messages électroniques, les compare aux listes noires anti-pollupostage actualisées sur Internet et peut ainsi réagir à un envoi massif de messages électroniques avant que les signatures antivirus correspondantes ne soient disponibles. La fonction OutbreakShield interroge sur Internet un très grand nombre de courriers électroniques suspects, ce qui lui permet de combler quasiment en temps réel la faille de sécurité entre le début d'un envoi massif de messages électroniques et son traitement au moyen de signatures antivirus spécialement adaptées. OutbreakShield est intégré à la fonction de blocage antivirus du courrier électronique.

Connexions chiffrées (SSL)

De nombreux fournisseurs de messagerie électronique (GMX, WEB.DE, T-Online et Freenet, par exemple) ont opté pour le chiffrement SSL. Ce protocole permet de renforcer clairement la sécurité des courriers et des messageries électroniques. Vous devez cependant également protéger vos courriers électroniques par le biais d'un programme antivirus. G Data vous propose pour cela le module Connexions chiffrées (SSL). Vous avez également la possibilité de vous assurer de l'absence de virus et de logiciels malveillants au niveau des courriers électroniques chiffrés SSL.

La vérification des courriers électroniques chiffrés SSL par le biais du logiciel G DATA nécessite l'importation d'un certificat du logiciel G DATA dans le programme de messagerie électronique. Vous avez ainsi l'assurance que votre logiciel G DATA peut vérifier les courriers électroniques entrants.

Tous les programmes de messagerie qui peuvent importer des certificats ou qui ont accès au magasin de certificats Windows sont pris en charge, comme :

- Outlook 2003 ou une version supérieure

- Thunderbird

- The Bat

- Pegasusmail

Veuillez procéder comme suit si le certificat G DATA n'est pas automatiquement installé :

1. Votre programme de messagerie électronique ne doit pas être activé lors de l'installation du certificat. Vous devez donc fermer tous les programmes de messagerie électronique avant de créer et d'installer le certificat.

2. Activez la case à cocher de vérification du logiciel G DATA en cas de connexions SSL.

3. Cliquez sur le bouton d'exportation du certificat. Le logiciel G DATA crée alors un certificat. Ce fichier porte le nom suivant : GDataRootCertificate.crt.

4. Ouvrez le fichier GDataRootCertificate.crt. Une boîte de dialogue vous permettant d'installer le certificat sur votre ordinateur s'affiche.

5. Dans la boîte de dialogue, cliquez sur le bouton **Installer le certificat** et suivez les consignes de l'assistant d'installation.

Vous avez terminé. Outlook et tous les autres programmes de messagerie électronique qui ont accès au magasin de certificats Windows reçoivent alors le certificat nécessaire pour s'assurer de l'absence de virus et autres logiciels malveillants dans les courriers électroniques chiffrés SSL.

Remarque : si vous utilisez **Thunderbird (portable)** et que le certificat n'est pas automatiquement importé, vous devez l'importer de nouveau et modifier les paramètres de confiance du certificat G DATA créé. Pour ce faire, veuillez sélectionner le bouton **Certificats** sous **Paramètres > Avancé > Certificats** dans Thunderbird (portable). Différents onglets apparaissent alors. Veuillez sélectionner l'onglet **Organismes de certification**, puis le bouton **Importer**. Vous pouvez ensuite sélectionner le certificat G DATA **G DATA Mail Scanner Root**.

Si vous activez la case à cocher des champs suivants et cliquez sur OK, votre messagerie Thunderbird portable est protégée par G DATA :

- **Faire confiance à cette autorité de certification pour identifier les sites Web**
- **Faire confiance à cette autorité de certification pour identifier les utilisateurs de la messagerie électronique**
- **Faire confiance à cette autorité de certification pour identifier les développeurs de logiciels**

D'autres programmes de messagerie électronique proposent des fonctions similaires pour l'importation de certificats. En cas de doute, veuillez vous reporter à l'aide correspondante pour déterminer la procédure à suivre pour le programme de messagerie électronique utilisé.

Avancé

Si votre programme de messagerie électronique n'utilise pas les ports standards, vous avez la possibilité, sous **Numéro de port du serveur**, d'indiquer le port utilisé pour les courriers électroniques entrants ou sortants. Cliquez sur le bouton **Par défaut** pour rétablir automatiquement les numéros de port standard. Vous pouvez également saisir plusieurs ports. Séparez ces derniers les uns des autres par une virgule.

Attention : Microsoft Outlook est protégé par un plugiciel spécial au moyen duquel vous pouvez vérifier directement dans Outlook les dossiers et les courriers électroniques. Pour analyser un courrier électronique ou un dossier dans Outlook, il vous suffit de cliquer sur l'icône G DATA. Le dossier sélectionné est alors soumis à une analyse antivirus.

Le logiciel traite les messages entrants avant le programme de messagerie. En présence de fichiers volumineux ou d'une connexion lente, il peut arriver que ce dernier affiche un message d'erreur parce qu'il ne peut pas accéder immédiatement aux données des messages, celles-ci étant en cours d'analyse par le logiciel. Si vous activez la case à cocher **Ne pas dépasser la limite de temps du serveur de messagerie**, ce message d'erreur ne s'affiche plus et dès que les données de la messagerie électronique sont soumises à une analyse antivirus, le logiciel les transmet tout à fait normalement au programme de messagerie électronique.

Analyses antivirus automatiques

Vous pouvez activer ou désactiver ici l'analyse en cas d'inactivité. Vous pouvez également vous assurer régulièrement (au lieu d'exécuter cette analyse ou en complément de cette analyse) de l'absence d'infections au niveau de votre ordinateur ou de parties de votre ordinateur. Vous pouvez ainsi procéder à de telles vérifications à des moments où vous n'utilisez pas l'ordinateur.

Vérifications antivirus programmées : il suffit souvent que l'ordinateur soit soumis à une analyse en cas d'inactivité. Le bouton **Nouveau** vous permet cependant de créer différentes analyses antivirus automatiques, indépendantes les unes des autres. On peut imaginer, par exemple, procéder chaque jour à une analyse du dossier Téléchargements et ne vérifier les fichiers MP3 qu'une fois par mois.

Le chapitre suivant vous indique comment créer des analyses antivirus personnalisées.

Généralités

Indiquez ici le nom de l'analyse antivirus automatique créée. Nous vous conseillons d'utiliser des noms évocateurs comme *Disques durs locaux (analyse hebdomadaire)* ou *Archives (analyse mensuelle)*.

Si vous cochez la case **Éteindre l'ordinateur à la fin de cette tâche**, votre ordinateur sera automatiquement mis hors tension à la fin de l'analyse antivirus automatique. Cela est utile lorsque vous souhaitez exécuter l'analyse antivirus après vos heures de travail.

Tâche : toute exécution de demande de vérification de l'ordinateur ou de parties de l'ordinateur est qualifiée de tâche.

Volume de l'analyse

Indiquez ici si la vérification antivirus doit être effectuée sur les disques durs locaux, si la mémoire et les zones de démarrage automatique doivent être testées ou si seuls certains répertoires et fichiers doivent être vérifiés. Le cas échéant, indiquez, à l'aide du bouton **Sélection**, les répertoires souhaités.

Sélectionner les répertoires/fichiers : Dans l'arborescence des répertoires, vous pouvez sélectionner et ouvrir des répertoires, dont le contenu sera ensuite affiché dans l'affichage des fichiers, en cliquant sur l'icône Plus. Tous les répertoires et fichiers dont la case à cocher est activée sont vérifiés par le logiciel. Les dossiers, dont certains des fichiers ne doivent pas être analysés, comporteront une marque grise.

Planification

Cet onglet vous permet de définir la fréquence des tâches correspondantes. Choisissez la fréquence sous **Exécuter**, puis définissez les paramètres correspondants sous **Date/Heure**. Si vous avez sélectionné l'option **Au démarrage du système**, il ne vous est pas nécessaire de définir un planning : le logiciel procède toujours à la vérification au redémarrage de l'ordinateur.

- **Exécuter la tâche si l'ordinateur n'était pas sous tension à l'heure de début** : si cette option est activée, les analyses antivirus automatiques non effectuées sont exécutées lorsque l'ordinateur est redémarré.

- **Ne pas exécuter en mode batterie** : afin de ne pas réduire inutilement la durée de fonctionnement de la batterie, vous pouvez définir, pour les ordinateurs portables par exemple, que les analyses antivirus automatiques n'ont lieu que lors de la connexion de l'ordinateur au réseau électrique.

Paramètres d'analyse

Cette rubrique vous permet de définir les paramètres de l'analyse antivirus automatique.

- **Utiliser les moteurs** : le logiciel fonctionne avec deux moteurs antivirus, deux programmes d'analyse antivirus optimisés. Sur les ordinateurs anciens et lents, l'utilisation d'un seul moteur permet d'accélérer la vérification antivirus mais en règle générale, il vous est recommandé de conserver le paramètre **Les deux moteurs**.

- **Fichiers infectés** : votre logiciel a détecté un virus ? Dans le cadre du paramètre par défaut, le logiciel vous demande ce que vous voulez faire avec le virus et le fichier infecté. Si vous souhaitez toujours réaliser la même action, vous pouvez procéder ici au réglage correspondant. Le paramètre **Désinfecter (sinon : envoyer en quarantaine)** offre, à ce titre, une sécurité optimale pour vos données.

- **Archives infectées** : indiquez ici si les fichiers d'archive (les fichiers avec l'extension RAR, ZIP ou encore PST, par exemple) ne doivent pas être traités comme les fichiers normaux. Nous attirons cependant votre attention sur le fait que le fait de placer une archive en quarantaine peut endommager celle-ci au point qu'elle ne puisse plus être utilisée, même une fois rétablie à son emplacement d'origine.

Définissez, en outre, en cliquant sur **Avancé**, les analyses supplémentaires devant être réalisées par l'outil de surveillance anti-virus.

Dans la plupart des cas cependant, l'utilisation des paramètres standard définis suffit largement.

- **Types de fichiers** : vous pouvez définir ici quels types de fichiers seront analysés par le logiciel G DATA.

- **Heuristique** : lorsque l'analyse heuristique est utilisée, les virus sont reconnus non seulement par le biais de la base de données des virus que vous obtenez à chaque mise à jour du logiciel, mais également au moyen de certaines caractéristiques typiques aux virus. Bien que ce paramètre ajoute à votre sécurité, il peut dans de rares cas déclencher une fausse alerte.

- **Vérifier les archives** : la vérification de données compressées dans des archives (on les reconnaît aux extensions de fichiers ZIP, RAR ou encore PST, par exemple) nécessite beaucoup de temps et s'avère généralement inutile lorsque la protection antivirus est activée au niveau du système. Lorsqu'une archive est décompressée, l'outil de surveillance reconnaît alors les virus jusqu'ici cachés et empêche automatiquement leur propagation.

- **Analyser les archives de courriers électroniques** : cette option vous permet de déterminer si les archives de messagerie doivent également être analysées.
- **Analyser les rubriques du système** : les différents volets comme les secteurs de démarrage ne doivent pas, normalement, être exclus du contrôle antivirus.
- **S'assurer de l'absence de composeurs/logiciels espions/logiciels publicitaires** : cette fonction permet de détecter les composeurs et autres logiciels nuisibles (logiciels espions, logiciels publicitaires et logiciels à risques). Il peut s'agir de programmes établissant des connexions Internet onéreuses contre votre gré, programmes qui n'ont rien à envier au potentiel financièrement dévastateur des virus : ils peuvent par ex. enregistrer discrètement vos habitudes de navigation, voire l'ensemble de vos saisies clavier (y compris vos mots de passe) puis, la première occasion venue, utiliser Internet pour les transmettre à un tiers.
- **Détecter les RootKits** : les trousses administrateur pirate tentent d'esquiver les méthodes de détection habituelles des virus. Un contrôle supplémentaire à la recherche de ces logiciels malveillants est toujours recommandé.
- **Inscrire dans le journal** : cette case à cocher vous permet d'indiquer que le logiciel doit créer un protocole lors de la vérification antivirus. Il est possible de le consulter ensuite dans la rubrique Protocoles.

Compte utilisateur

Vous définirez ici le compte utilisateur sur lequel l'analyse antivirus sera effectuée. Ce compte sera nécessaire pour l'accès au lecteur réseau.

AntiSpam

Filtre anti-spam

Le filtre anti-pollupostage vous propose de nombreux paramètres vous permettant de bloquer de manière efficace les courriers électroniques contenant des contenus indésirables ou provenant d'expéditeurs indésirables (expéditeurs de masse, par exemple). Le programme vérifie de nombreux critères des courriers électroniques de pollupostage types. Ces différents critères évalués résultent en une valeur qui reflète leur probabilité d'être du courrier indésirable. Le bouton **Utiliser le filtre antispam** vous permet d'activer ou de désactiver le filtre anti-pollupostage.

Pour activer ou désactiver les différents types de filtres anti-pollupostage, activez ou désactivez la case à cocher à côté de l'entrée correspondante. Pour modifier les différents filtres, il vous suffit de cliquer sur l'entrée correspondante. Une boîte de dialogue permettant de modifier les paramètres s'affiche. Les options suivantes sont disponibles :

- **OutbreakShield anti-spam** : la technologie OutbreakShield permet de détecter et de combattre les programmes malveillants dans les envois massifs de messages électroniques avant que les signatures virales correspondantes ne soient disponibles. La fonction OutbreakShield interroge sur Internet un très grand nombre de courriers électroniques suspects, ce qui lui permet de combler quasiment en temps réel le laps de temps entre le début d'un envoi massif de courriers électroniques et son traitement au moyen de signatures antivirus adaptées. Si vous utilisez un ordinateur placé derrière un serveur proxy, cliquez sur le bouton **Options Internet** lors de la configuration et procédez aux modifications correspondantes. Modifiez ces options uniquement si OutbreakShield ne fonctionne pas.
- **Utiliser liste blanche** : La liste blanche vous permet d'exclure explicitement de la vérification des spams les adresses de certains expéditeurs ou de certains domaines. Pour ce faire, il vous suffit de saisir, dans le champ **Adresses/domaines**, les adresses électroniques (*lettre d'information@site d'information.fr*, par exemple) ou les domaines (*site d'information.fr*, par exemple) que vous ne souhaitez pas prendre en compte dans le cadre de la suspicion de pollupostage. Le logiciel G DATA ne traite alors pas les courriers électroniques de l'expéditeur ou du domaine d'expéditeurs comme du pollupostage.

  Le bouton **Importer** vous permet d'ajouter à la liste blanche des listes prédéfinies d'adresses électroniques ou de domaines. Les adresses et les domaines de ces listes doivent se présenter l'un en-dessous de l'autre dans des lignes individuelles. Le format utilisé est celui d'un simple fichier texte, pouvant, par exemple, être créé avec l'outil Bloc-notes de Windows. Le bouton **Exporter** vous permet d'exporter une telle liste blanche sous la forme d'un fichier texte.
- **Utiliser liste noire** : la liste noire vous permet de définir explicitement comme étant du pollupostage les messages provenant des adresses de certains expéditeurs ou de certains domaines. Pour ce faire, il vous suffit de saisir, dans le champ **Adresses/domaines**, les adresses électroniques (*lettre d'information@megaspam.fr.vu*, par exemple) ou les domaines (*megaspam.fr.vu*, par exemple) que vous souhaitez prendre en compte dans le cadre de la suspicion de pollupostage. Le logiciel G DATA traite alors les courriers électroniques de l'expéditeur ou du domaine d'expéditeurs comme des courriers présentant une probabilité élevée de pollupostage. Le bouton **Importer** vous permet d'ajouter à la liste noire des listes prédéfinies d'adresses électroniques ou de domaines. Les adresses et les domaines de ces listes doivent se présenter l'un en-dessous de l'autre dans des lignes individuelles. Le format utilisé est celui d'un simple fichier texte, pouvant, par exemple, être créé avec l'outil Bloc-notes de Windows. Le bouton **Exporter** vous permet d'exporter la liste noire en tant que fichier texte.

- **Utiliser listes noires en temps réel (paramètre standard)** : vous pouvez trouver sur Internet des listes noires contenant les adresses IP de serveurs connus pour envoyer du pollupostage. Le logiciel G DATA formule des requêtes auprès des listes noires en temps réel afin de déterminer si le serveur expéditeur est répertorié. Si tel est le cas, la probabilité Spam augmente. Il est généralement recommandé ici d'utiliser les paramètres par défaut ; vous avez cependant la possibilité d'assigner aux listes noires 1, 2 et 3 vos propres adresses issues d'Internet.

- **Utiliser des mots clés (corps du message)** : la liste des mots-clés vous permet d'utiliser les mots du texte des courriers électroniques dans le cadre de la suspicion de pollupostage. Si au moins un des termes est présent dans le texte du message, la probabilité d'être en présence d'un spam augmente. Cette liste peut être modifiée à volonté à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**. Le bouton **Importer**vous permet également d'ajouter des listes prédéfinies de mots-clés. Les entrées figurant dans ces listes doivent se présenter l'un au-dessous de l'autre dans des lignes individuelles. Le format utilisé est celui d'un simple fichier texte, pouvant, par exemple, être créé avec l'outil Bloc-notes de Windows. Le bouton **Exporter** vous permet d'exporter une telle liste de mots-clés sous la forme d'un fichier texte. La case à cocher **Ne rechercher que parmi les termes entiers** vous permet d'ordonner au logiciel G DATA de rechercher uniquement des mots entiers dans la ligne d'objet d'un message.

- **Utiliser des mots clés (objet)** : la liste des mots-clés vous permet également d'utiliser les mots de la ligne d'objet des courriers dans le cadre de la suspicion de pollupostage. Si au moins un des termes est présent dans la ligne d'objet, la probabilité de pollupostage augmente.

- **Utiliser filtrage de contenu** : le filtre de contenu est un filtre intelligent qui calcule la probabilité de pollupostage à partir des mots utilisés dans le corps du message. Ce filtre ne se contente pas de travailler avec des listes exhaustives de mots : il étoffe ses connaissances à chaque nouveau courrier électronique réceptionné. Le bouton **Rechercher dans contenu des tableaux** permet d'afficher les listes de mots utilisées par le filtre de contenu pour classer un courrier électronique dans la catégorie pollupostage. Le bouton **Rétablir les tableaux initiaux** permet de supprimer tous les contenus de tableau appris, le filtre de contenu recommence alors la procédure d'apprentissage depuis le début.

Réaction

La section Réaction vous permet de choisir le comportement du filtre anti-pollupostage face aux courriers électroniques suspectés d'être du pollupostage. Vous pouvez définir à cette occasion trois barèmes rendant compte du degré de probabilité de pollupostage des courriers électroniques concernés déterminé par le logiciel G DATA.

- **Soupçon spam** : cette option permet de définir le mode de traitement des courriers électroniques dans lesquels le logiciel G DATA détecte des éléments de pollupostage. Les messages classés ici ne sont pas forcément du pollupostage, il peut parfois s'agir de lettres d'information ou de mailings souhaités par le destinataire. Il est recommandé ici de signaler au destinataire que le message est suspecté d'être un spam.

- **Probabilité élevée de spam** : rassemble les courriers électroniques associant de nombreuses marques distinctives du pollupostage. Il s'agit très rarement de messages souhaités par le destinataire.

- **Probabilité très élevée de spam** : les courriers électroniques qui remplissent tous les critères du pollupostage sont regroupés ici. Il ne s'agit ici en aucun cas de courriers électroniques souhaités et le rejet de ce type de messages est recommandé dans la plupart des cas.

Ces trois types de menace peuvent être paramétrés individuellement. Il vous suffit de cliquer sur le bouton **Modifier** et de définir la réaction du logiciel G DATA. L'option **Refuser le message** vous donne ainsi la possibilité de ne même pas voir arriver ces courriers électroniques dans votre boîte de réception. L'option **Insérer l'avertissement de spam dans l'objet et le texte du message** vous permet d'identifier les courriers électroniques caractérisés comme étant du pollupostage. Cela vous permet par exemple de mieux les trier. Si vous utilisez**Microsoft Outlook** (attention : ne confondez pas cette application avec Outlook Express ou Windows Mail), vous avez également la possibilité de déplacer les courriers électroniques suspectés de pollupostage dans un dossier paramétrable à volonté de votre boîte de réception (**Déplacer message vers dossier**). Vous pouvez créer ce dossier via le logiciel G DATA, en définissant le dossier correspondant sous **Nom du dossier**.

> **Remarque** : même si vous n'utilisez pas Outlook, vous avez la possibilité de déplacer dans un dossier les messages reconnus comme étant du pollupostage. Ajoutez un avertissement dans la ligne d'objet (par exemple, *[Spam]*) et créez dans votre programme de messagerie électronique une règle qui déplacera les messages dans un autre dossier grâce au texte se trouvant dans la ligne d'objet.

Paramètres avancés

Cette rubrique vous permet de modifier en détail la reconnaissance du pollupostage par le logiciel G DATA et de l'adapter en fonction des messages électroniques. Il est toutefois recommandé d'utiliser les paramètres standard dans la majorité des cas. Ne modifiez les paramètres avancés que si vous maîtrisez le sujet et savez exactement ce que vous faites.

Autres filtres

Les filtres suivants sont réglés ici de manière ordinaire. Vous pouvez si nécessaire les désactiver en supprimant la coche.

- **Désactiver les scripts HTML**
- **Filtrage des pièces jointes dangereuses**

Vous pouvez créer de nouvelles règles de filtrage à l'aide du bouton **Nouveau** ou modifier des filtres existants à l'aide du bouton **Modifier**. Les filtres créés figurent dans la liste et peuvent être cochés ou décochés pour leur activation ou désactivation à gauche de chaque entrée. Si un filtre est coché, il est alors activé. Si un filtre est décoché, il est alors désactivé. Pour supprimer définitivement un filtre, sélectionnez-le d'un clic de souris et cliquez ensuite sur le bouton **Supprimer**.

Les possibilités de filtrage qui sont mises à votre disposition ici concernent des filtres supplémentaires, qui complètent le filtre anti-pollupostage du logiciel G DATA et vous simplifient le paramétrage. Le filtre anti-pollupostage vous propose de nombreux paramètres vous permettant de bloquer de manière efficace les courriers électroniques contenant des contenus indésirables ou provenant d'expéditeurs indésirables (expéditeurs de masse, par exemple). Le programme vérifie de nombreux critères des courriers électroniques de pollupostage types. Ces différents critères évalués résultent en une valeur qui reflète leur probabilité d'être du courrier indésirable. Vous disposez de plusieurs onglets où tous les paramètres pertinents sont classés par thèmes.

Lorsque vous créez un filtre, une fenêtre de sélection s'affiche et vous demande de déterminer le type de filtres de base. Vous pouvez ainsi saisir toutes les données supplémentaires de filtre à créer dans une fenêtre d'assistance adaptée à ce type de filtre. Vous pouvez très aisément installer des filtres contre toute sorte de danger.

- **Désactiver les scripts HTML** : ce filtre permet de désactiver les scripts dans la partie HTML du courrier électronique. Si les scripts sont utiles sur les sites Internet, ils sont plutôt gênants dans un message électronique au format HTML. Dans certains cas, les scripts HTML sont également activement utilisés pour infecter des ordinateurs. Les scripts peuvent se propager à partir de l'ouverture d'un document infecté mais également dès l'affichage en aperçu d'un courrier électronique.
- **Filtrage des pièces jointes dangereuses** : les filtres des pièces jointes vous offrent un grand nombre de possibilités de blocage des pièces jointes. La plupart des virus des courriers électroniques se propagent via ce type de pièces jointes qui contiennent dans la plupart des cas des fichiers exécutables plus ou moins bien dissimulés. Il peut s'agir ici de simples fichiers .exe contenant un programme nuisible, mais également de scripts VB, se dissimulant parfois même dans des fichiers images, des films ou des musiques soi-disant sûrs. Les utilisateurs doivent prendre toutes les précautions avant d'exécuter une pièce jointe. En cas de doutes, il est préférable de demander confirmation à l'expéditeur avant d'exécuter un fichier suspect.

  Vous pouvez répertorier les extensions de fichier auxquelles le filtre doit être appliqué sous **Extensions de fichier**. Vous pouvez regrouper dans un filtre tous les fichiers exécutables (les fichiers EXE et COM, par exemple), mais vous pouvez également filtrer d'autres formats (MPEG, AVI, MP3, JPEG, JPG, GIF, etc.) au cas où leur taille surchargerait votre serveur de messagerie électronique. Vous pouvez bien évidemment aussi filtrer les fichiers d'archive (ZIP, RAR ou CAB). Séparez toutes les extensions de fichier d'un groupe de filtrage par un point-virgule.

  La fonction **Filtrer également les pièces jointes des courriers intégrés** vous permet de filtrer les pièces jointes sélectionnées sous **Extensions de fichier**, même dans les courriers électroniques qui constituent eux-mêmes une pièce jointe. Cette option doit en règle générale être activée.

  Avec l'option **Ne renommer que les pièces jointes**, les pièces jointes ne sont pas automatiquement supprimées, mais simplement renommées. Cela peut s'avérer utile dans le cas de fichiers exécutables (comme les fichiers EXE et COM), mais aussi de fichiers Microsoft Office, pouvant éventuellement renfermer des scripts et des macros exécutables. En renommant les pièces jointes, vous évitez toute appréciation hâtive qui amènerait l'utilisateur à ouvrir la pièce jointe sans réfléchir. Avant de pouvoir l'utiliser, le destinataire du message doit d'abord enregistrer la pièce jointe et éventuellement la renommer. Si l'option **Ne renommer que les pièces jointes** n'est pas activée, les pièces jointes correspondantes sont tout simplement supprimées.

  Le champ **Suffixe** vous permet de définir la chaîne de caractères à ajouter à l'extension de fichier initiale et d'empêcher l'exécution d'un fichier d'un simple clic (par exemple, exe_danger). Grâce au champ **Insérer le texte suivant dans le message**, vous pouvez informer le destinataire du courrier électronique filtré qu'une pièce jointe a été supprimée ou renommée suite à une règle de filtrage.
- **Filtrage du contenu** : Grâce au filtrage du contenu, vous pouvez facilement bloquer des messages abordant un sujet particulier ou contenant des mots particuliers.

Il vous suffit de saisir, sous **Critères de recherche**, les mots-clés et les expressions qui doivent faire réagir le logiciel G DATA. Vous pouvez également combiner les textes à votre guise en vous servant des opérateurs logiques ET et OU.

Sous **Domaine de recherche**, indiquez les zones du courrier électronique dans lesquelles ces expressions doivent être recherchées. L'**en-tête** d'un message inclut notamment les adresses électroniques de l'expéditeur et du destinataire, la ligne d'objet, ainsi que des informations relatives aux données d'expédition, aux protocoles et aux programmes utilisés. **Objet** ne vérifie que le contenu de la ligne de l'objet sans se préoccuper d'autres informations textuelles de l'en-tête. Vous pouvez également, pour le **corps du message**, limiter le domaine de recherche aux seuls messages texte ou au texte des courriers HTML (texte HTML).

Vous pouvez déterminer, sous **Messages intégrés**, si la recherche du filtre de contenu s'étend également aux courriers électroniques en pièce jointe du message reçu.
Vous pouvez déterminer dans **Réaction** comment réagir face aux courriers électroniques que le logiciel G DATA détecte en tant que pollupostage. L'option **Refuser le message** permet au programme de messagerie électronique de ne pas recevoir les courriers électroniques concernés.

Si vous activez la case à cocher **Insérer avertissement dans les champs objet et corps du message**, le texte de la ligne d'objet peut présenter un avertissement (préfixe dans la ligne d'objet), comme par exemple *Pollupostage* ou *Attention*. Vous pouvez également saisir un texte qui sera placé avant le texte d'origine du courrier électronique en cas de soupçon de pollupostage (Message dans texte).

Si vous utilisez *Microsoft Outlook* (**attention** : ne confondez pas cette application avec Outlook Express ou Outlook Mail), vous avez également la possibilité de déplacer les courriers électroniques suspectés de pollupostage dans un dossier paramétrable à volonté de votre boîte de réception (**Déplacer message vers dossier**). Vous pouvez créer ce dossier via le logiciel G DATA, en définissant le dossier correspondant sous **Nom du dossier**.

- **Filtrage de l'expéditeur** : Grâce au filtrage de l'expéditeur, vous pouvez facilement bloquer les messages provenant d'expéditeurs particuliers. Pour ce faire, il vous suffit de saisir, sous **Expéditeurs/Domaines**, les adresses électroniques ou les noms de domaine qui doivent faire réagir le logiciel G DATA. Vous pouvez saisir plusieurs entrées en les séparant par des points-virgules.

Vous pouvez déterminer dans **Réaction** comment réagir face aux courriers électroniques que le logiciel G DATA détecte en tant que pollupostage.

L'option **Refuser le message** permet au programme de messagerie électronique de ne pas recevoir les courriers électroniques concernés.

Si vous activez la case à cocher **Insérer avertissement dans les champs objet et corps du message**, le texte de la ligne d'objet peut présenter un avertissement (préfixe dans la ligne d'objet), comme par exemple *Pollupostage* ou *Attention*. Vous pouvez également saisir un texte qui sera placé avant le texte d'origine du courrier électronique en cas de soupçon de pollupostage (Message dans texte).

Si vous utilisez *Microsoft Outlook* (**attention** : ne confondez pas cette application avec Outlook Express ou Windows Mail), vous avez également la possibilité de déplacer les courriers électroniques suspectés de pollupostage dans un dossier paramétrable à volonté de votre boîte de réception (**Déplacer message vers dossier**). Vous pouvez créer ce dossier via le logiciel G DATA, en définissant le dossier correspondant sous **Nom du dossier**.

- **Filtrage langues** : le filtrage langues vous permet de définir automatiquement certaines langues comme du pollupostage. Normalement, si vous n'êtes en contact avec aucun correspondant anglophone, vous pouvez définir tout message en anglais comme du pollupostage, ce qui vous épargnera de nombreux courriers indésirables. Il vous suffit de sélectionner les langues dont vous n'attendez pas de messages réguliers. Le logiciel G DATA peut ainsi augmenter considérablement la détection de pollupostage concernant ces courriers électroniques.

Vous pouvez déterminer dans **Réaction** comment réagir face aux courriers électroniques que le logiciel G DATA détecte en tant que pollupostage.

L'option **Refuser le message** permet au programme de messagerie électronique de ne pas recevoir les courriers électroniques concernés.

Si vous activez la case à cocher **Insérer avertissement dans les champs objet et corps du message**, le texte de la ligne d'objet peut présenter un avertissement (préfixe dans la ligne d'objet), comme par exemple *Pollupostage* ou *Attention*. Vous pouvez également saisir un texte qui sera placé avant le texte d'origine du courrier électronique en cas de soupçon de pollupostage (Message dans texte).

Si vous utilisez *Microsoft Outlook* (**attention** : ne confondez pas cette application avec Outlook Express ou Windows Mail), vous avez également la possibilité de déplacer les courriers électroniques suspectés de pollupostage dans un dossier paramétrable à volonté de votre boîte de réception (**Déplacer message vers dossier**). Vous pouvez créer ce dossier via le logiciel G DATA, en définissant le dossier correspondant sous **Nom du dossier**.

Autre

Vous avez la possibilité de définir d'autres paramètres dans cette zone.

- **Vérifier les messages reçus non lus lors du démarrage du programme** : *Uniquement pour Microsoft Outlook* : cette option permet de détecter le pollupostage. Lorsque vous ouvrez l'application Outlook, tous les courriers électroniques non lus de la boîte de réception et des sous-dossiers du logiciel G DATA sont vérifiés.

- **Autres logiciels de messagerie (POP3)** : pour des raisons techniques, les courriers électroniques reçus via le protocole POP3 ne peuvent pas être directement supprimés. Si un des filtres refuse un courrier électronique, il est remplacé par un texte de remplacement standard. Le texte de remplacement des courriers électroniques refusés est le suivant : **Courriel refusé**. Vous pouvez toutefois paramétrer individuellement cette fonctionnalité d'avertissement. Vous disposez des caractères génériques suivants (définis par un signe %, puis une lettre minuscule) pour le texte du champ **Objet** et le **texte du courrier électronique** :

  %s Expéditeur

  %u Objet

Vous pouvez définir dans votre programme de messagerie une règle de suppression automatique des courriers électroniques incluant le texte de remplacement indiqué ici.

Pare-feu

Automatisation

Si vous ne souhaitez pas vous occuper du pare-feu, vous devez conserver le paramètre Automatique. Parallèlement au mode de pilote automatique, qui constitue sans aucun doute le meilleur choix pour un grand nombre d'utilisateurs, vous disposez d'une multitude d'options qui vous permettent de configurer le pare-feu G DATA de manière optimale, en fonction de vos besoins et de vos exigences.

Les paramètres du pare-feu regroupent deux rubriques de base, qui peuvent être configurées de manière individuelle :

Pilote automatique

Vous pouvez indiquer ici si le pare-feu fonctionne de manière autonome et intelligente et ne demande pas l'avis de l'utilisateur pour bloquer ou autoriser les requêtes Internet ou si l'utilisateur est interrogé en cas de doutes.

- **Mode pilote automatique** : Le pare-feu travaille ici de manière entièrement autonome et tient les dangers automatiquement à distance de votre ordinateur domestique. Cette option offre une protection intégrale très pratique et est recommandée dans la plupart des cas.

- **Création manuelle des règles** : si vous souhaitez configurer votre pare-feu de manière personnalisée, la création manuelle de règles vous permet de définir la protection du pare-feu en fonction de vos besoins.

- **Proposer le mode pilote automatique au lancement d'une application en plein écran** : avec les jeux sur ordinateur (et autres applications plein écran), le pare-feu peut perturber le fil du jeu ou son affichage à cause de ses nombreuses questions. Afin de garantir un plaisir de jeu absolu sans baisse de sécurité, le pilote automatique constitue un paramètre judicieux car il bloque les requêtes du pare-feu. Si vous n'utilisez pas le pilote automatique par défaut, vous pouvez veiller, via cette fonction, à ce qu'il soit toujours proposé lorsque vous utilisez un programme en mode plein écran.

Paramètres de sécurité définis par l'utilisateur

Quand vous utilisez votre ordinateur, le pare-feu note au fur et à mesure les programmes que vous utilisez pour accéder à Internet et ceux qui présentent ou pas un risque pour la sécurité du système. Avec les niveaux de sécurité prédéfinis, vous pouvez adapter le pare-feu à vos besoins personnels sans travail administratif ni connaissances techniques dans le domaine de la sécurité réseau. Il vous suffit de faire glisser le curseur vers le niveau de sécurité souhaité. Le programme met à votre disposition les niveaux de sécurité suivants :

- **Sécurité optimale** : Les règles du pare-feu sont définies sur la base de paramètres très fins. Vous devez pour cela maîtriser les notions techniques de la technologie réseau (TCP, UDP, ports, etc.). Le pare-feu détecte les moindres écarts par rapport aux règles et vous pose de nombreuses questions pendant la phase d'apprentissage.

- **Sécurité élevée** : Les règles du pare-feu sont définies sur la base de paramètres très fins. Vous devez pour cela maîtriser les notions techniques de la technologie réseau (TCP, UDP, ports, etc.). Le pare-feu peut vous poser de nombreuses questions dans certains cas.

- **Sécurité normale** : Les règles du pare-feu sont uniquement définies au niveau des applications. Les assistants n'affichent pas les

détails relatifs aux réseaux. Pendant la phase d'apprentissage, les questions qui vous sont posées sont limitées au minimum.

- **Sécurité peu élevée** : Les règles du pare-feu sont uniquement définies au niveau des applications. Les assistants n'affichent pas les détails relatifs aux réseaux et très peu de questions vous sont posées pendant la phase d'apprentissage. Ce niveau de sécurité maintient une protection maximale contre les demandes de connexion entrante.

- **Pare-feu désactivé** : Vous pouvez également désactiver le pare-feu si nécessaire. Dans ce cas, votre ordinateur reste connecté à Internet et aux autres réseaux, mais n'est plus protégé par le pare-feu contre les attaques ou les tentatives d'espionnage.

Si vous souhaitez définir des paramètres particuliers pour le pare-feu, activez la case à cocher **Paramètres de sécurité définis par l'utilisateur**. Vous devez pour cela disposer d'un minimum de connaissances dans le domaine de la sécurité réseau.

Interroger

Vous déterminez ici quand, comment et si le pare-feu doit prévenir l'utilisateur dès que des programmes demandent l'établissement d'une connexion à Internet ou à un réseau.

Créer une règle

Si le pare-feu établit une connexion réseau, une boîte d'informations s'affiche, dans laquelle vous pouvez indiquer comment procéder avec l'application en cours. Vous pouvez définir ici la mesure appliquée précisément lors de l'acceptation ou du refus d'un accès réseau :

- **Par application** : l'accès réseau est autorisé ou interdit de manière générale sur chaque port et avec chaque protocole de transfert (par exemple, TCP ou UDP) pour l'application affichée.

- **Par protocole/port/application** : L'application demandant un accès au réseau obtient l'autorisation de se connecter en ligne uniquement avec le protocole de transmission sollicité et exclusivement avec le port auquel la requête a été adressée. Si la même application demande un autre accès au réseau sur un autre port ou avec un autre protocole, la question réapparaît et une autre règle de ce type peut être créée.

- **Par application, si au moins x demandes à traiter** : il existe des applications (Microsoft Outlook, par exemple) qui, lors d'une demande réseau, exigent plusieurs ports ou utilisent plusieurs protocoles à la fois. Le paramètre Par protocole/port/application activé, plusieurs questions vous sont posées. Vous pouvez donc accorder aux applications une autorisation ou un refus global pour l'utilisation du réseau dès que la connexion est autorisée ou bloquée par l'utilisateur.

Applications de serveur inconnues

Les applications qui ne sont pas encore gérées par une règle du pare-feu peuvent être traitées de manière différente. Le moment de la demande de connexion est assez aléatoire. Si l'application serveur fonctionne en réception, cela signifie qu'elle attend une demande de connexion en mode de veille. Sinon, la demande ne survient que lorsque la connexion a réellement lieu.

Identification des réseaux non protégés

Bien entendu, un pare-feu ne peut fonctionner correctement que si tous les réseaux auxquels les ordinateurs à protéger accèdent sont reconnus et surveillés. Vous devez donc impérativement laisser l'identification des réseaux non protégés activée.

Questions répétées au sujet des applications

Vous pouvez renouveler vos tentatives de connexion pour une certaine application. Ainsi, lorsque vous essayez de vous connecter sans avoir établi de règles spécifiques, la question n'apparaîtra pas constamment, mais par exemple toutes les 20 secondes ou à des intervalles que vous pouvez vous-même définir.

Test de référence

Lors de la recherche des références des applications pour lesquelles l'accès au réseau a été autorisé par le pare-feu, une somme de contrôle est calculée sur la base de la taille des fichiers et d'autres critères. Si la somme de contrôle du programme change soudainement, il est possible que le programme ait été modifié par un programme nuisible. Dans ce cas, le pare-feu déclenche une alarme.

Vérification de référence pour les modules chargés : cette option permet de contrôler les applications, mais également les modules utilisés par les applications (bibliothèques de liens dynamiques, par exemple). Étant donné que ces modules changent souvent et que de nouveaux modules sont régulièrement chargés, un test cohérent portant sur les références modifiées et inconnues des modules peut nécessiter un temps d'administration considérable. Chaque module modifié déclenche une question de sécurité de la part du pare-feu. Le test des modules ne doit donc être utilisé de cette manière que lorsque les exigences en matière de sécurité sont particulièrement élevées.

Autre

D'autres options de paramétrage sont ici disponibles.

Paramètres pour l'assistant de règles

Vous pouvez indiquer ici si les nouvelles règles doivent être créées à l'aide de l' Assistant de règles ou en mode de modification avancé. Pour les utilisateurs ne maîtrisant pas le thème de la sécurité réseau, nous recommandons l'utilisation de l'assistant de règles.

Vérifications au démarrage du programme

Vous pouvez déterminer ici si le pare-feu doit rechercher les applications de serveur inconnues à chaque démarrage du programme. Cette fonction de recherche doit toujours être activée, sauf si vous travaillez au sein d'un réseau fermé.

Enregistrer le protocole de connexion



Vous pouvez définir ici la durée de conservation des données de connexion par le pare-feu. Vous pouvez conserver les données jusqu'à 60 heures et les consulter sous la rubrique Protocoles.

Tuner

Généralités

Vous pouvez définir ici les paramètres suivants :

- **Effacer les données restaurées** : vous pouvez indiquer ici quand les données de restauration (créées par le logiciel G DATA en cas de modifications) doivent être supprimées.
- **Effacer les anciennes données** : vous pouvez indiquer ici quand les anciennes données (ancien dossier TEMP, par exemple) doivent être supprimées.
- **Effacer les raccourcis du bureau** : vous pouvez indiquer ici quand les raccourcis bureau inutiles (non utilisés depuis un certain nombre de jours) doivent être supprimés.
- **Rechercher également des mises à jour Office lors d'une mise à jour Microsoft** : vous pouvez indiquer ici si le tuner doit automatiquement rechercher des mises à jour Office en plus des mises à jour Windows sur Internet. La mise à jour des deux éléments permet de gagner du temps, vous êtes également ainsi à jour sur le plan de la sécurité. La recherche de mises à jour Office ne peut naturellement fonctionner que si Microsoft Office est installé sur votre ordinateur.
- **Ne pas créer de journal avec les informations détaillées sur les éléments supprimés** : Le tuner est conçu pour garder en mémoire les informations complètes de toutes les modifications effectuées. si vous considérez un fichier journal incluant des informations au sujet des éléments supprimés par le tuner comme un risque pour la sécurité, vous pouvez empêcher la création du protocole de suppression.
- **Supprimer les fichiers temporaires de manière permanente** : cette fonction vous permet d'exclure les fichiers Web (cookies, données Internet temporaires, par exemple) de l'option de restauration du tuner. Ces fichiers ne peuvent alors pas être restaurés. Si vous activez cette fonction, vous réduisez considérablement la quantité de fichiers que le tuner doit conserver dans la section de restauration. Il en résulte des améliorations de performance.
- **Proscrire le redémarrage automatique de l'ordinateur par l'intermédiaire de ce service** : cette option vous permet d'empêcher l'éventuel redémarrage de l'ordinateur que lancerait le tuner en cas de procédure de réglage programmée. Étant donné que le Tuner n'effectuerait un redémarrage d'ordinateur non sollicité que dans le cas où aucun utilisateur ne serait identifié, il est donc recommandé de ne pas activer ce paramètre dans la plupart des cas.
- **Permettre la création de points de restauration individuels** : sans cette fonction, le logiciel G DATA ne peut plus effectuer aucune restauration.
- **Ne pas prendre en compte le type de lecteur lors de la défragmentation** : la plupart des fabricants ne conseillent pas de défragmenter leurs disques SSD, la défragmentation de ce type de disques durs est donc exclue par défaut dans G DATA Tuner. Si les lecteurs du logiciel G DATA ne peuvent pas être normalisés automatiquement, mais que vous avez la certitude que votre ordinateur ne contient pas de lecteurs SSD, vous pouvez laisser cette case à cocher activée. Lors de chaque exécution, le Tuner défragmente alors tous les disques durs du système.

Configuration

Cette rubrique vous permet de sélectionner tous les modules que le tuner doit utiliser lors des réglages. Les modules sélectionnés sont à cette occasion soit démarrés par une action automatique à fréquence déterminée (voir chapitre **Planification**) soit par une action manuelle. Un double-clic sur un module vous permettra de l'activer. Vous pouvez optimiser chacune des grandes rubriques de réglage suivantes :

- *Sécurité*: différentes fonctions qui téléchargent automatiquement des données à partir d'Internet, ne concernent que le fournisseur. Souvent, ces fonctions laissent entrer des logiciels nuisibles (malware). Grâce à ces modules, votre système est protégé et actualisé au maximum.

- *Performance*: les fichiers temporaires comme les copies de sécurité, les protocoles et les données d'installation qui occupent de l'espace de stockage mais ne sont plus utilisés après installation peuvent ralentir votre disque dur. De plus, ils occupent un espace de stockage non négligeable. Les processus et les icones de fichiers qui ne sont plus utilisés peuvent par ailleurs notoirement ralentir votre système. Les modules répertoriés ici vous permettront de libérer votre ordinateur de ces éléments encombrants superflus et d'accélérer ses performances.

- *Protection des données*: les modules qui se chargent de la protection de vos données sont regroupés ici. Les traces indésirables provenant de votre parcours sur Internet ou du mode d'utilisation de votre ordinateur qui peuvent trahir des informations sensibles et des mots de passe importants peuvent être effacées ici.

Protection du dossier

Cet onglet vous permet d'exclure certains dossiers (votre partition Windows, par exemple) de la suppression automatique des anciens fichiers.



Pour ce faire, il vous suffit de cliquer sur l'icône **Ajouter** et de sélectionner le dossier ou le lecteur correspondant.



Pour supprimer un répertoire d'exceptions, sélectionnez le répertoire dans la liste affichée et cliquez sur le bouton **Supprimer**.

Protection du fichier

La fonction Protection du fichier vous permet de protéger certains fichiers de la suppression par le tuner, comme les scores réalisés dans des jeux informatiques ou d'autres fichiers similaires à extension inhabituelle, pouvant être considérés comme des fichiers de sauvegarde ou temporaires.



Pour protéger certains fichiers, il suffit de cliquer sur le bouton **Ajouter** et d'indiquer le nom de fichier en question. Vous pouvez également travailler ici avec des caractères génériques.

Les caractères de remplacement fonctionnent comme suit :

- L'icône en forme de point d'interrogation (?) représente des caractères uniques.
- L'astérisque (*) remplace des suites de caractères.

Par exemple, pour protéger tous les dossiers .sav, saisissez *.sav. Pour protéger les fichiers de différents types mais de début de nom similaire, tapez par exemple « text *.*»

Veuillez à présent choisir le dossier dont vous souhaitez protéger les fichiers en cliquant sur le bouton Avancé. Sélectionnez maintenant le support d'enregistrement où se trouvent les fichiers à protéger. Le tuner protègera désormais les fichiers définis uniquement dans ce dossier (parties sauvegardées d'un dossier de jeu, par exemple).



Pour désactiver la protection d'un fichier, sélectionnez le fichier dans la liste affichée et cliquez sur le bouton **Supprimer**.

Planification

Via l'onglet **Planification horaire**, vous pouvez définir quand et à quelle fréquence la tâche de réglage automatique doit avoir lieu.

Sous l'option **Tous les jours**, vous pouvez indiquer, en saisissant les jours de la semaine, si l'ordinateur doit procéder au réglage uniquement les jours de la semaine, tous les deux jours ou le week-end, lorsque vous ne travaillez pas. Pour modifier les dates et les heures définies sous **Date/heure**, il vous suffit de sélectionner l'élément que vous souhaitez modifier (par exemple, le jour, l'heure, le mois ou l'année) à l'aide de la souris et de déplacer l'élément sur la frise chronologique à l'aide des touches fléchées ou de l'icône en forme de flèche située à droite du champ de saisie.

Si vous ne souhaitez procéder à aucun réglage automatique, il vous suffit de désactiver la case à cocher **Activé** pour l'exécution automatique des réglages.

Contrôle des périphériques

Le contrôle des périphériques vous permet de définir les supports mémoire autorisés en lecture et/ou en écriture sur votre ordinateur. Vous pouvez également empêcher le transfert de données privées sur une clé USB ou leur gravure sur un CD. De plus, vous pouvez indiquer précisément les supports de données amovibles (clés USB ou disques durs USB externes, par exemple) sur lesquels les données peuvent être téléchargées. Vous pouvez ainsi utiliser votre disque dur USB pour la sauvegarde de données sans que les autres disques durs aient accès à ces données.

Pour utiliser le contrôle des périphériques, vous devez activer la case à cocher **Activer le contrôle des périphériques** et sélectionner les périphériques pour lesquels les limitations sont définies :

- **Supports de données amovibles (clés USB, par exemple)**
- **Lecteurs de CD/DVD**
- **Lecteurs de disquettes**

Vous avez maintenant la possibilité de définir des règles pour les différents supports mémoire.

Règle générale

Vous pouvez indiquer que le périphérique ne doit pas du tout être utilisé (**Bloquer l'accès**), que les données peuvent être téléchargées du support, mais ne peuvent être enregistrées sur le support (**Accès en lecture**) ou qu'il n'existe aucune limitation pour le périphérique (**Accès complet**). La règle s'applique alors à tous les utilisateurs de votre ordinateur.

Règle spécifique à l'utilisateur

Si vous souhaitez que seuls certains utilisateurs disposent de droits limités pour les supports mémoire, vous pouvez sélectionner dans cette rubrique le nom d'utilisateur des autres utilisateurs enregistrés au niveau de votre ordinateur, puis limiter l'accès aux supports mémoire comme indiqué sous **Règle générale**. Vous disposez ainsi, en tant qu'administrateur et propriétaire de l'ordinateur, d'un accès complet tandis que les autres utilisateurs ne bénéficient que de droits limités.

Sélectionnez l'utilisateur. Lorsque vous cliquez sur OK, une boîte de dialogue, dans laquelle vous pouvez définir le type d'accès souhaité pour l'utilisateur et indiquer si les droits de l'utilisateur sont limités dans le temps (deux semaines, par exemple) (**Validité**), s'affiche.

> **Remarque** : Les règles spécifiques à l'utilisateur prévalent sur les règles générales. Ainsi, si vous déterminez que l'accès aux clés USB est interdit en règle générale, vous pouvez toutefois autoriser un utilisateur spécifique à utiliser les clés USB via une règle spécifique. Si un utilisateur dispose de certaines restrictions d'accès limitées dans le temps via le contrôle des périphériques, une fois les restrictions arrivées à expiration, la règle générale s'applique de nouveau pour cet utilisateur.

Règle spécifique au périphérique

Lors de l'utilisation de supports de données amovibles, tels que des clés USB ou des disques durs externes, vous pouvez également déterminer que seuls des supports de données amovibles définis peuvent accéder à votre ordinateur. Pour ce faire, connectez le support de données amovible à votre ordinateur et cliquez sur le bouton **Ajouter**. Vous pouvez sélectionner le support de données amovible souhaité dans la boîte de dialogue qui s'affiche. Lorsque vous cliquez sur OK, une boîte de dialogue, dans laquelle vous pouvez définir le type d'accès souhaité pour le support de données et indiquer si les droits d'utilisation du support de données sont limités dans le temps (deux semaines, par exemple) (**Validité**) et si tous les utilisateurs peuvent utiliser le support de données, s'affiche.

Sauvegarde

Cette rubrique vous permet de définir les paramètres généraux de fonctionnement du module de sauvegarde.

- **Répertoire pour les fichiers temporaires** : indiquez ici où les données temporaires du module de sauvegarde doivent être enregistrées. Ces fichiers sont créés lors de la sauvegarde ou de la restauration d'une sauvegarde, elles sont cependant automatiquement supprimées une fois le processus effectué. Vous devez toutefois disposer de suffisamment d'espace mémoire sur le disque dur, faute de quoi la vitesse de sauvegarde et de restauration est limitée. Ce paramètre ne doit être modifié que si l'espace mémoire disponible au niveau du répertoire sélectionné pour les fichiers temporaires est insuffisant.

- **Vérification du lecteur source/de destination sur le même disque dur** : le module de sauvegarde avertit normalement toujours l'utilisateur en cas de création d'une sauvegarde sur le support de données sur lequel se trouvent les fichiers d'origine. Ce, parce qu'en cas de panne/perte du support de données, la sauvegarde n'est plus disponible non plus. Si vous souhaitez néanmoins procéder aux sauvegardes régulières sur le support des données d'origine, vous pouvez désactiver le message d'avertissement.

Protocoles

Il existe des fonctions de protocoles pour les différents modules. Ces fonctions vous permettent de disposer d'une vue d'ensemble sur les actions effectuées par le logiciel G DATA pour vous protéger.

Protocoles de protection antivirus

La rubrique Journaux présente la liste des journaux créés par le logiciel. Les titres de colonne **Heure de démarrage**, **Type**, **Titre** et **État** vous permettent de trier les journaux selon les critères correspondants. Les boutons **Enregistrer sous** et **Imprimer** vous permettent d'enregistrer les fichiers journaux sous forme de fichiers texte ou de les imprimer. Pour supprimer un protocole, sélectionnez l'entrée du tableau à l'aide de la souris et appuyez sur la touche Suppr ou cliquez sur le bouton **Supprimer**.

Protocoles de pare-feu

La rubrique des protocoles crée, pour chaque action du pare-feu, un fichier journal complet. Vous pouvez y ouvrir les rapports d'actions spécifiques en double-cliquant sur le nom des actions. Vous pouvez également imprimer ces rapports ou les enregistrer sous forme de fichiers texte. Veuillez également lire à ce propos le chapitre **Paramètres : Autre**.

Protocoles de sauvegarde

La rubrique Protocoles prépare un fichier journal détaillé pour chaque action et chaque tâche de sauvegarde. Vous pouvez y ouvrir les rapports d'actions spécifiques en double-cliquant sur le nom des actions. Vous pouvez également imprimer ces rapports ou les enregistrer sous forme de fichiers texte. Veuillez également lire à ce propos le chapitre **Sauvegarder et rétablir**.

Protocoles de contrôle parental

La rubrique Journaux permet à l'administrateur de consulter toutes les tentatives de consultation des contenus bloqués par les autres utilisateurs. Sélectionnez dans la liste déroulante l'utilisateur dont vous voulez consulter le protocole. Veuillez également lire à ce propos le chapitre **Paramètres : Protocole**.

> **Remarque** : Vous pouvez bien évidemment également supprimer ces protocoles en cliquant sur le bouton **Supprimer le journal**.

Protocole de contrôle des périphériques

La rubrique Protocole crée un fichier journal complet pour chaque action du gestionnaire de périphériques. Reportez-vous à ce titre au chapitre suivant : **Paramètres : Contrôle des périphériques**

Foire aux questions : BootScan

Si votre ordinateur est tout neuf ou s'il était jusqu'à présent protégé par un logiciel antivirus, vous pouvez procéder à l'installation comme suit.

Si vous avez des raisons de penser que votre ordinateur est infecté, nous vous recommandons de procéder, avant installation du logiciel, à une analyse BootScan.

> **Analyse BootScan** : lorsque vous démarrez votre ordinateur, le système d'exploitation Windows démarre normalement automatiquement. Cette opération s'appelle l'amorçage. Il est cependant également possible de démarrer automatiquement d'autres systèmes d'exploitation et d'autres programmes.
>
> G DATA vous propose, en plus de la version Windows, une version spéciale, vous permettant de procéder à une analyse antivirus de votre ordinateur avant le lancement de Windows.

Configuration requise

L'analyse BootScan vous permet de lutter contre les virus qui se sont infiltrés dans votre ordinateur avant l'installation du logiciel antivirus.

Il existe en effet une version spéciale du logiciel qui peut être exécutée avant le lancement de Windows.

Démarrage à partir du CD/DVD-ROM : veuillez procéder comme suit si votre ordinateur ne démarre pas à partir du CD/DVD-ROM :

1. Éteignez votre miniportatif.

2. Redémarrez votre ordinateur. Pour accéder au programme de configuration BIOS, vous devez généralement appuyer sur la touche Suppr (ou sur la touche F2 ou F10, selon le système) lors du démarrage de l'ordinateur.

3. Les modalités de modification en détail des paramétrages de votre BIOS varient d'un ordinateur à l'autre.

   Veuillez consulter la documentation de votre ordinateur.

   En conséquence, la succession logique d'un amorçage devrait être **CD/DVD-ROM, C**, c'est-à-dire que le lecteur de CD/DVD-ROM devient le **premier dispositif de démarrage** et la partition du disque dur avec son système d'exploitation Windows, **le deuxième**.

4. Enregistrez les modifications et redémarrez votre ordinateur. Votre ordinateur est maintenant prêt pour un BootScan.

   Comment annuler une analyse BootScan ? Inutile de vous inquiéter si, après un redémarrage, votre ordinateur n'affiche pas l'environnement Windows habituel, mais l'interface du logiciel BootScan de G DATA.

   Si vous n'avez planifié aucune analyse BootScan, il vous suffit de sélectionner l'entrée **Microsoft Windows** à l'aide des touches fléchées et de cliquer sur **Return**. Windows démarre alors normalement, sans analyse BootScan préalable.

   Démarrer à partir d'une clé USB : si vous utilisez une clé USB en tant que support d'amorçage, vous pouvez également la sélectionner en tant que premier périphérique d'amorçage.

Foire aux questions : fonctions du programme

Icône de sécurité

Votre logiciel G DATA protège en permanence votre ordinateur contre les virus et les logiciels malveillants. Afin que vous puissiez constater que la protection est active, une icône s'affiche dans la barre des tâches, à côté de l'horloge.



Cette icône G DATA indique que tout fonctionne correctement et que la protection est activée sur votre ordinateur.



Si la protection antivirus a été désactivée ou si d'autres problèmes apparaissent, l'icône G DATA affiche un signal d'avertissement. Il faut alors, dans la mesure du possible, démarrer rapidement le logiciel G DATA et vérifier les paramètres.



Une icône spécifique est également utilisée lorsque le logiciel G DATA procède à un téléchargement de données Internet.

Si vous cliquez sur cette icône avec le bouton droit de la souris, il s'affiche un menu contextuel qui vous permet de paramétrer les fonctionnalités de sécurité principales du logiciel.

Différentes fonctions sont disponibles à partir des boutons suivants :

- **Lancer le logiciel G DATA** : vous permet d'activer le SecurityCenter et de définir les paramètres de la protection antivirus. Vous pourrez lire à quoi sert le SecurityCenter dans le chapitre : **SecurityCenter**
- **Désactiver le gardien** : vous permet de désactiver et de réactiver la protection antivirus. Ceci peut s'avérer utile si vous devez, par exemple, copier des fichiers volumineux d'un dossier de votre disque dur d'un emplacement à un autre ou lancer des procédures gourmandes en mémoire (copier des DVD, par exemple). Nous vous conseillons de ne pas désactiver la protection antivirus plus que nécessaire et, dans la mesure du possible, de ne pas vous connecter à Internet ou de ne pas lire de nouvelles données non vérifiées (sur CD, DVD, cartes mémoire, clés USB, etc.) pendant ce temps.
- **Désactiver le pare-feu** : si vous utilisez une version du logiciel G DATA avec pare-feu intégré, vous pouvez désactiver le pare-feu dans le menu contextuel. Dans ce cas, votre ordinateur reste connecté à Internet et aux autres réseaux, mais n'est plus protégé par le pare-feu contre les attaques ou les tentatives d'espionnage.
- **Désactiver le pilote automatique** : le pilote automatique est un élément du pare-feu qui décide de manière entièrement autonome des requêtes et contacts que votre ordinateur doit accepter sur le réseau ou sur Internet. Le pilote automatique est optimal pour une utilisation normale et vous devriez le laisser toujours connecté. Tout comme le pare-feu, le pilote automatique est disponible dans certaines versions du logiciel G DATA.
- **Mettre les signatures antivirus à jour** : votre logiciel antivirus doit toujours être actualisé. Vous pouvez évidemment exécuter l'actualisation des données automatiquement depuis le logiciel. Si vous deviez cependant avoir un besoin vital d'une actualisation, vous pouvez la démarrer à l'aide du bouton **Mettre les signatures antivirus à jour**. Vous lirez en quoi une mise à jour antivirus est nécessaire au chapitre : **Analyse antivirus**
- **Statistiques** : vous pouvez afficher ici des statistiques au sujet des vérifications effectuées par l'outil de surveillance mais également des informations concernant les analyses d'inactivité, les messages du filtre Web et d'autres paramètres.

Exécuter l'analyse antivirus

L'analyse antivirus vous permet d'analyser votre ordinateur et de détecter des attaques conduites par des logiciels nuisibles. Lorsque vous démarrez l'analyse antivirus, celle-ci contrôle chaque fichier de votre ordinateur afin de voir s'il est en mesure d'infecter d'autres fichiers ou s'il est lui-même déjà infecté.

Si, lors d'une analyse antivirus, des virus ou d'autres logiciels malveillants sont détectés, il existe différentes possibilités de supprimer ou de neutraliser les virus.

1 Démarrez l'analyse antivirus. La procédure vous est expliquée au chapitre **Protection antivirus**

2 Votre ordinateur est analysé à la recherche d'une attaque de virus potentielle. Une fenêtre s'ouvre alors contenant des informations sur le statut de l'analyse.

Une barre de progression, dans la partie supérieure de la fenêtre, vous indique l'avancée de la vérification du système. Vous avez, pendant la vérification antivirus, différentes possibilités pour influencer son déroulement :

- **En cas de surcharge du système, mettre l'analyse antivirus en pause** : grâce à ce champ, l'analyse antivirus est uniquement lancée lorsque les autres activités en cours au niveau de l'ordinateur sont terminées.
- **Éteindre l'ordinateur après l'analyse antivirus** : cette fonction est très pratique lorsque vous procédez à l'analyse antivirus la nuit ou après le travail. Une fois la vérification antivirus du logiciel G DATA terminée, l'ordinateur s'éteint.
- **Archives protégées par mot de passe** : dans la mesure où une archive est protégée par un mot de passe, le logiciel G DATA ne peut analyser les fichiers de l'archive. Si vous validez l'option, le programme affiche la liste des archives protégées par mot de passe qu'il n'a pas pu vérifier. Tant que celle-ci n'est pas décompressée, le virus qu'elle contient éventuellement ne présente aucun risque pour votre système.
- **Accès refusé** : sous Windows, il existe des fichiers utilisés exclusivement par certaines applications et ne peuvent donc pas être analysés tant que ces applications sont en cours. C'est pourquoi, il est préférable de quitter toutes les autres applications avant de lancer une analyse antivirus. Si vous validez cette option, le programme affiche la liste des fichiers qui n'ont pas pu être vérifiés.

3a Si votre système n'est pas infecté, vous pouvez quitter la fenêtre de l'assistant, une fois la vérification terminée, en cliquant sur le bouton **Fermer**. Votre système a été soumis à une analyse antivirus et n'est pas infecté.

3b Si des virus et autres programmes malveillants sont détectés, vous avez maintenant la possibilité d'indiquer ce que vous souhaitez faire des virus trouvés. Il suffit généralement de cliquer sur le bouton **Exécuter des actions**.

Le logiciel G DATA utilise alors un paramètre standard (dans la mesure où vous n'avez pas modifié les paramètres sous **Paramètres : Analyse antivirus manuelle** pour les archives et les fichiers infectés) et désinfecte les fichiers contaminés. Les fichiers sont réparés de manière à pouvoir être de nouveau utilisés sans aucune restriction et à ne plus présenter aucun risque pour l'ordinateur.

S'il n'est pas possible de procéder à une désinfection, le fichier est placé en quarantaine. Il est chiffré et placé dans un dossier sécurisé, de manière à ne plus occasionner aucun dommage.

Si vous avez encore besoin des fichiers infectés, vous pouvez, de manière exceptionnelle, les retirer de la quarantaine et les utiliser.

Votre système a fait l'objet d'une analyse antivirus et n'est pas infecté.

3c Une fois les fichiers/objets infectés identifiés, vous pouvez déterminer les fichiers dont vous n'avez plus besoin. Vous pouvez également appliquer des mesures différentes en fonction de chaque virus trouvé.

Dans la liste des virus détectés, vous pouvez définir, pour chaque fichier infecté, l'action à effectuer, dans la colonne Action.

- **Protocoles uniquement** : l'infection est recensée au niveau de l'écran **Protocoles**. Une réparation ou une suppression des fichiers concernés n'a cependant pas lieu. **Attention** : si un virus n'est que journalisé, il demeure actif et dangereux.
- **Désinfecter (sinon : uniquement enregistrer l'événement)** : le programme essaie ici de supprimer le virus d'un fichier infecté ; si cela se révèle impossible sans endommager le fichier, le virus est enregistré et vous pouvez vous en occuper ultérieurement, via l'entrée du fichier journal. *Attention ! si un virus n'est que journalisé, il demeure actif et dangereux.*
- **Désinfecter (sinon : mettre en quarantaine)** : il s'agit du paramètre standard. Le programme essaie ici de supprimer le virus d'un fichier infecté ; si cela se révèle impossible sans endommager le fichier, le fichier est mis en **Quarantaine**. Veuillez également lire à ce propos le chapitre : **Fichiers en quarantaine**
- **Désinfecter (sinon : Supprimer le fichier)** : le programme essaie ici de supprimer le virus du fichier infecté. Si ce n'est pas possible, le fichier est supprimé. Il est recommandé de n'utiliser cette fonction que si votre ordinateur ne contient pas de données importantes. Une suppression ciblée des fichiers infectés peut conduire, dans le pire des cas, à ce que Windows ne fonctionne plus et à ce qu'une réinstallation s'impose.
- **Mettre le fichier en quarantaine** : les fichiers infectés sont envoyés directement en Quarantaine. Dans la quarantaine, les fichiers sont sauvegardés sous forme cryptée. Le virus est ainsi hors d'état de nuire et il est toujours possible de soumettre le fichier infecté à une tentative éventuelle de réparation. Veuillez également lire à ce propos le chapitre : **Fichiers en quarantaine**
- **Supprimer le fichier** : Il est recommandé de n'utiliser cette fonction que si votre ordinateur ne contient pas de données importantes. Une suppression ciblée des fichiers infectés peut conduire, dans le pire des cas, à ce que Windows ne fonctionne plus et à ce qu'une réinstallation s'impose.

Lorsque vous cliquez sur le bouton **Exécuter les actions**, le logiciel G DATA traite les différents virus détectés de la manière indiquée.

Votre système fait l'objet d'une analyse antivirus. Si vous utilisez un paramètre avec l'option **Enregistrer l'événement**, il est possible que votre ordinateur soit encore infecté.

Alarme antivirus

Si le logiciel G DATA détecte un virus ou un autre programme malveillant sur votre ordinateur, une fenêtre d'avertissement s'affiche dans le coin de l'écran.

Vous disposez alors des possibilités suivantes pour traiter le fichier infecté.

- **Protocoles uniquement** : l'infection est recensée au niveau de l'écran Protocoles mais une réparation ou une suppression des fichiers concernés n'a pas lieu. Vous pouvez cependant analyser séparément les virus détectés par le biais de la rubrique Protocole et les supprimer de manière ciblée. *Attention ! si un virus n'est que journalisé, il demeure actif et dangereux.*

- **Désinfecter (sinon : envoyer en quarantaine)** : Le programme essaie ici de supprimer le virus d'un fichier infecté ; si cela se révèle impossible sans endommager le fichier, le fichier est mis en Quarantaine. Veuillez également lire à ce propos le chapitre : Comment la quarantaine fonctionne-t-elle ?

- **Mettre le fichier en quarantaine** : les fichiers infectés sont envoyés directement en Quarantaine. Dans la quarantaine, les fichiers sont sauvegardés sous forme cryptée. Le virus est ainsi hors d'état de nuire et il est toujours possible de soumettre le fichier infecté à une tentative éventuelle de réparation. Veuillez également lire à ce propos le chapitre : **Fichiers en quarantaine**

- **Supprimer le fichier infecté** : Il est recommandé de n'utiliser cette fonction que si votre ordinateur ne contient pas de données importantes. Une suppression ciblée des fichiers infectés peut conduire, dans le pire des cas, à ce que Windows ne fonctionne plus et à ce qu'une réinstallation s'impose.

> **Quarantaine et boîtes aux lettres de messagerie électronique** : il existe des fichiers pour lesquels la mise en quarantaine est déconseillée (fichiers d'archive des boîtes aux lettres de messagerie électronique, par exemple). Lorsqu'une boîte aux lettres de messagerie électronique est mise en quarantaine, votre programme de messagerie ne peut plus y accéder et il risque de ne plus fonctionner. Vous devez redoubler de prudence en ce qui concerne les ***fichiers avec l'extension PST***, car ils contiennent généralement des données de votre boîte de messagerie électronique Outlook.

Alarme pare-feu

Si des programmes et des processus inconnus souhaitent se connecter au réseau, le pare-feu en mode de création manuelle de règles demande généralement s'il doit les autoriser ou les refuser. Il ouvre alors une boîte de dialogue d'informations contenant des informations détaillées sur l'application concernée. Vous pouvez autoriser ou interdire à l'application l'accès au réseau de manière unique ou permanente. Si vous autorisez ou refusez l'accès d'un programme de manière permanente, une règle est ajoutée au jeu de règles du réseau et le programme ne génère plus d'alertes.

Les boutons suivants sont à votre disposition :

- **Toujours autoriser** : ce bouton crée une règle pour l'application concernée (par exemple, Opera.exe, Explorer.exe ou iTunes.exe) qui autorise l'accès à Internet ou au réseau de manière permanente. Cette règle est définie comme règle générée sur demande sous la rubrique Ensembles de règles.

- **Autoriser provisoirement** : Ce bouton autorise l'application concernée à n'accéder qu'une seule fois au réseau. À la tentative d'accès suivante de l'application, le pare-feu affichera de nouveau une alerte.

- **Toujours refuser** : ce bouton crée une règle pour l'application concernée (par exemple, dialer.exe, spam.exe ou trojan.exe) qui lui interdit d'accéder à Internet ou au réseau de manière permanente. Cette règle est définie comme règle générée sur demande sous la rubrique Ensembles de règles.

- **Refuser provisoirement** : Ce bouton vous permet d'interdire une seule fois l'accès au réseau de l'application concernée. À la tentative d'accès suivante de l'application, le pare-feu affichera de nouveau une alerte.

Vous obtenez par ailleurs des informations sur le protocole, le port et l'adresse IP avec lesquels l'application concernée doit interagir.

Message not-a-virus

Les fichiers accompagnés de la mention not-a-virus signalent des applications potentiellement dangereuses. De tels programmes ne disposent pas directement de fonctions malveillantes mais pourraient cependant dans certaines circonstances être utilisés contre vous par des auteurs d'attaques. Font par exemple partie de cette catégorie certains programmes d'administration à distance, les programmes de basculement automatique de l'affectation du clavier, les clients IRC, les serveurs FTP ou divers programmes de service pour la création ou le camouflage de procédures.

Désinstallation

Si vous souhaitez désinstaller le logiciel G DATA de votre ordinateur, veuillez procéder à la désinstallation via le panneau de configuration de votre système d'exploitation. La désinstallation s'effectue automatiquement.

Si, pendant la désinstallation, vous disposez encore de fichiers en quarantaine dans le logiciel G DATA, une boîte de dialogue vous demandera si vous souhaitez ou non les supprimer. Si vous choisissez de ne pas les supprimer, ils seront transférés dans un dossier G DATA spécial et verrouillé de votre ordinateur afin de ne causer aucun dommage. Ces fichiers ne peuvent être de nouveau traités qu'une fois le logiciel G DATA réinstallé sur votre ordinateur.

Lors de la désinstallation, le système vous demande si vous souhaitez supprimer les paramètres et journaux. Si vous ne supprimez pas ces fichiers, les journaux et les paramètres seront à nouveau à votre disposition lors d'une réinstallation du logiciel.

Pour finaliser la désinstallation, cliquez sur le bouton **Terminer**. Le logiciel est maintenant complètement désinstallé de votre système.

Foire aux questions : questions portant sur les licences

Licences multipostes

Avec une licence multipostes, vous pouvez utiliser le logiciel G DATA sur le nombre d’ordinateurs indiqué dans la licence. Après l'installation sur le premier ordinateur et la mise à jour Internet, vous recevez des codes d'accès transmis en ligne. Si vous installez maintenant votre logiciel sur un autre ordinateur, il vous suffit de saisir le nom d’utilisateur et le mot de passe que vous avez reçus lors de l’enregistrement sur le serveur de mise à jour G DATA. Répétez le procédé pour tous les autres ordinateurs.

Veuillez utiliser, sur l’ensemble des PC, les données d’accès (nom d’utilisateur et mot de passe) pour la mise à jour Internet qui vous ont été attribuées lors de votre première inscription. Pour ce faire, procédez comme suit :

1. Lancez le logiciel G DATA.
2. Sous **SecurityCenter**, cliquez sur **Mettre les signatures antivirus à jour**.
3. Veuillez saisir dans la fenêtre qui s'affiche maintenant les codes d'accès que vous avez reçus auparavant par courriel. La licence de l'ordinateur est enregistrée lorsque vous cliquez sur **OK**.

Prolongation de la licence

Quelques jours avant l'expiration de votre licence, une fenêtre d'informations s'affiche dans la barre des tâches. Si vous cliquez dessus, une boîte de dialogue qui vous permet de prolonger votre licence sans problème et en quelques étapes s’affiche. Il vous suffit de cliquer sur le bouton **Acheter maintenant** et de saisir les données vous concernant. Votre protection antivirus est alors immédiatement garantie. Vous recevrez la facture, dans les jours suivants, par la poste.

Remarque : Cette boîte de dialogue ne s’affiche qu’au bout de la première année. Votre licence G DATA est ensuite automatiquement prolongée chaque année. Vous pouvez toutefois résilier à tout moment cet abonnement sans fournir aucune raison.

Changement d’ordinateur

Vous pouvez utiliser le logiciel G DATA sur un nouvel ordinateur ou sur un autre ordinateur à l’aide de vos données d’accès existantes. Il vous suffit d’installer le logiciel et de saisir les données d’accès. Le serveur de mise à jour établit alors la connexion au nouvel ordinateur. Si le logiciel G DATA est encore installé sur votre ancien ordinateur, la licence doit être transférée de l’ancien ordinateur vers le nouvel ordinateur.

Remarque : Le nombre de transmissions de licence est limité. Lorsque la valeur limite est atteinte, la licence est bloquée : il n’est plus possible de charger aucune mise à jour.

Copyright

Index